

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-249899
(43)Date of publication of application : 14.09.2001

(51)Int.Cl.
G06F 15/00
G06F 13/00
G06F 17/60
H04Q 7/38
H04L 9/32
H04L 12/66

(21)Application number : 2000-062213

(71)Applicant : SONY CORP

(22)Date of filing : 07.03.2000

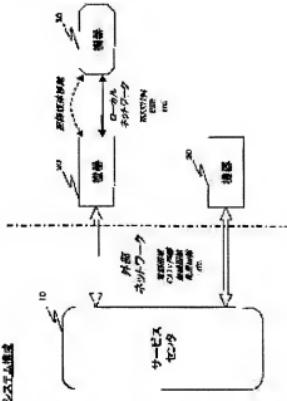
(72)Inventor : ISHIBASHI YOSHITO
ASANO TOMOYUKI
OKA MAKOTO

(54) SERVICE PROVIDING SYSTEM VIA COMMUNICATION MEANS, ITS METHOD, SERVICE MEDIATING DEVICE AND PROGRAM PROVIDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To realize a service providing system by which maintenance and control via an external network concerning an electronic unit without having a communication part and a cipher processing part are performed by keeping a communication secret.

SOLUTION: A controlled unit (low-order unit) being the object of maintenance or control, etc., is constituted to transfer data to a high-order unit via a local network or via an information recording medium such as a memory stick. The high-order unit is provided with a communication means to transfer data received from a service center to the controlled unit (low-order unit) via the local network or the information recording medium. In the high-order unit, the safety of communication data is guaranteed since a communication processing is performed with the service center after enciphering data so that important information such as control information or individual information required for providing control information is prevented from being leaked.



LEGAL STATUS

[Date of request for examination] 21.12.2006

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

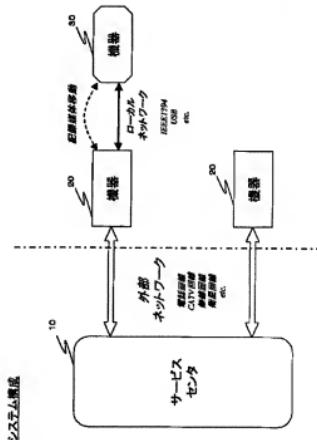
(51)Int.Cl. G 0 6 F 15/00	識別記号 3 3 0	F I G 0 6 F 15/00	テ-ゴ-1- (参考) 3 3 0 A 5 B 0 4 9 3 3 0 Z 5 B 0 8 5
	3 2 0 13/00		3 2 0 A 5 B 0 8 9 3 5 1 3 5 7
		13/00	3 5 1 Z 5 J 1 0 4 3 5 7 A 5 K 0 3 0
		審査請求 未請求 請求項の数26 O L (全 85 頁)	最終頁に続く

(21)出願番号 特願2000-62213(P2000-62213)	(71)出願人 000002185 ソニー株式会社 東京都品川区北品川6丁目7番35号
(22)出願日 平成12年3月7日(2000.3.7)	(72)発明者 石橋 義人 東京都品川区北品川6丁目7番35号 ソニ ー株式会社内
	(72)発明者 浅野 智之 東京都品川区北品川6丁目7番35号 ソニ ー株式会社内
	(74)代理人 100101801 弁理士 山田 英治 (外2名)
	最終頁に続く

(54)【発明の名称】 通信手段を介したサービス提供システム、サービス提供方法、およびサービス仲介装置、並びに
(57)【要約】 プログラム提供媒体

【課題】 通信部、暗号処理部を持たない電子機器に対する外部ネットワークを介したメンテナンス、制御を通信の秘密を保持して可能とするサービス提供システムを実現する。

【解決手段】 メンテナンス、制御等の対象である制御対象機器（下位機器）を上位機器にローカルネットワークを介して、あるいはメモリスティック等の情報記録媒体を介してデータ転送可能な構成とする。上位機器は通信手段を有し、サービスセンタから受信したデータをローカルネットワークまたは情報記録媒体を介して制御対象機器（下位機器）に転送する。上位機器はデータを暗号化した上でサービスセンタと通信処理を実行するため、通信データの安全性が保証され、制御情報、あるいは制御情報を提供するために必要となる個人情報などの重要な情報の漏洩が防止される。



【特許請求の範囲】

【請求項 1】ローカルネットワークインタフェース手段、または情報記録媒体インタフェース手段の少なくともいずれかを有する制御対象機器、
外部ネットワークに対するインタフェース手段と、該外部ネットワークを使用した転送データの暗号処理を実行する暗号処理手段とを有するとともに、前記制御対象機器のローカルネットワークインタフェース手段または情報記録媒体インタフェース手段のいずれかを介して前記制御対象機器に対してデータ転送可能な構成を有する上位機器とを有し、
前記上位機器は、前記外部ネットワークを介して前記制御対象機器に対する制御情報をサービスセンタから受信して、該受信制御情報をローカルネットワークまたは情報記録媒体を介して前記制御対象機器に転送する構成を有することを特徴とする通信手段を介したサービス提供システム。

【請求項 2】前記サービスセンタおよび前記上位機器は認証処理手段を有し、前記サービスセンタおよび前記上位機器間のデータ送受信は、認証処理による認証が成立した場合にのみ実行する構成であることを特徴とする請求項 1 に記載の通信手段を介したサービス提供システム。

【請求項 3】前記上位機器および前記制御対象機器は認証処理手段を有し、前記上位機器および前記制御対象機器間のデータ送受信は、認証処理による認証が成立した場合にのみ実行する構成であることを特徴とする請求項 1 に記載の通信手段を介したサービス提供システム。

【請求項 4】前記上位機器および前記制御対象機器は認証処理手段を有し、前記上位機器および前記制御対象機器間における前記情報記録媒体を介したデータ転送は、前記上位機器および前記制御対象機器による前記情報記録媒体の認証処理による認証が成立した場合にのみ実行する構成であることを特徴とする請求項 1 に記載の通信手段を介したサービス提供システム。

【請求項 5】前記サービスセンタは前記上位機器および制御対象機器の機器識別子を登録した機器情報データベースを有し、該機器情報データベースに登録された機器識別子と、前記上位機器または制御対象機器から受信する機器識別子との照合処理を実行することにより、機器正当性検証処理を実行する構成を有することを特徴とする請求項 1 に記載の通信手段を介したサービス提供システム。

【請求項 6】前記サービスセンタは、前記上位機器および制御対象機器の利用者識別子を登録した利用者情報データベースを有し、該利用者情報データベースに登録された利用者識別データと、前記上位機器または制御対象機器から受信する利用者識別データとの照合処理を実行することにより、利用者正当性検証処理を実行する構成を有することを特徴とする請求項 1 に記載の通信手段を

介したサービス提供システム。

【請求項 7】前記サービスセンタおよび前記上位機器において送受信されるデータは、当該通信セッションでのみ有効なセッション鍵を用いて暗号化処理がなされたデータであることを特徴とする請求項 1 に記載の通信手段を介したサービス提供システム。

【請求項 8】前記上位機器および前記制御対象機器において転送されるデータは、当該通信セッションでのみ有効なセッション鍵を用いて暗号化処理がなされたデータであることを特徴とする請求項 1 に記載の通信手段を介したサービス提供システム。

【請求項 9】前記サービスセンタは前記制御対象機器に対して、機器診断処理、機器修復処理、データバックアップ処理、データリストア処理、データ配信処理、ヘルプデータ提供処理、操作情報提供処理のいずれかのサービスを提供する構成であることを特徴とする請求項 1 に記載の通信手段を介したサービス提供システム。

【請求項 10】前記サービスセンタおよび前記上位機器間の認証処理は、公開鍵暗号方式によって実行し、前記上位機器および前記制御対象機器間の認証処理は、公開鍵暗号方式または共通鍵暗号方式のいずれかの方式によって実行する構成であることを特徴とする請求項 1 に記載の通信手段を介したサービス提供システム。

【請求項 11】前記サービスセンタおよび前記上位機器間のデータ通信は、共通鍵暗号方式によって実行し、前記上位機器および前記制御対象機器間のデータ通信は、共通鍵暗号方式によって実行する構成であることを特徴とする請求項 1 に記載の通信手段を介したサービス提供システム。

【請求項 12】制御対象機器に対する制御情報を通信手段を介して提供するサービス提供方法であり、サービスセンタから、該サービスセンタと通信手段を介して接続される上位機器に対して暗号処理のなされた制御情報を送信するデータ送信ステップと、前記上位機器の受信した暗号化制御情報を、暗号化制御情報としてまたは前記上位機器において復号した復号制御情報としてローカルネットワークインタフェースまたは情報記録媒体を介して前記制御対象機器に転送するデータ転送ステップと、
を有することを特徴とするサービス提供方法。

【請求項 13】前記サービスセンタから前記上位機器に対するデータ送信ステップの前に、前記サービスセンタと前記上位機器間での認証処理を実行する認証処理ステップを有し、前記データ送信ステップは、前記認証処理ステップにおける認証が成立した場合にのみ実行することを特徴とする請求項 12 に記載の通信手段を介したサービス提供方法。

【請求項 14】前記上位機器から前記制御対象機器に対するデータ転送ステップの前に、

前記上位機器と前記制御対象機器間での認証処理を実行する認証処理ステップを有し、

前記データ転送ステップは、前記認証処理ステップにおける認証が成立した場合にのみ実行することを特徴とする請求項1 2に記載の通信手段を介したサービス提供方法。

【請求項1 5】前記上位機器と前記制御対象機器間でのデータ転送が情報記録媒体を介したデータ転送として行われる場合において、前記上位機器および前記制御対象機器による前記情報記録媒体の認証処理を実行する認証処理ステップを有し、前記データ転送ステップは、前記認証処理ステップにおける認証が成立した場合にのみ実行することを特徴とする請求項1 2に記載の通信手段を介したサービス提供方法。

【請求項1 6】前記サービスセンタは前記上位機器および制御対象機器の機器識別子を登録した機器情報データベースを有し、該機器情報データベースに登録された機器識別子と、前記上位機器または制御対象機器から受信する機器識別子との照合処理による機器正当性検証処理ステップを実行することを特徴とする請求項1 2に記載の通信手段を介したサービス提供方法。

【請求項1 7】前記サービスセンタは、前記上位機器および制御対象機器の利用者識別子を登録した利用者情報データベースを有し、該利用者情報データベースに登録された利用者識別データと、前記上位機器または制御対象機器から受信する利用者識別データとの照合処理による利用者正当性検証処理ステップを実行することを特徴とする請求項1 2に記載の通信手段を介したサービス提供方法。

【請求項1 8】前記サービスセンタまたは前記上位機器のいずれかは、相互に送受信するデータを暗号化する鍵として、当該通信セッションでのみ有効なセッション鍵を生成し、

前記暗号処理は、生成したセッション鍵による暗号化処理として実行することを特徴とする請求項1 2に記載の通信手段を介したサービス提供方法。

【請求項1 9】前記上位機器または前記制御対象機器のいずれかは、相互に送受信するデータを暗号化する鍵として、当該通信セッションでのみ有効なセッション鍵を生成し、

前記暗号処理は、生成したセッション鍵による暗号化処理として実行することを特徴とする請求項1 2に記載の通信手段を介したサービス提供方法。

【請求項2 0】前記サービスセンタは前記制御対象機器に対して、機器診断処理、機器修復処理、データパックアップ処理、データリストア処理、データ配信処理、ヘルプデータ提供処理、操作情報提供処理のいずれかのサービスを提供することを特徴とする請求項1 2に記載の通信手段を介したサービス提供方法。

【請求項2 1】前記サービスセンタおよび前記上位機器間の認証処理は、公開鍵暗号方式によって実行し、前記上位機器および前記制御対象機器間の認証処理は、公開鍵暗号方式または共通鍵暗号方式のいずれかの方式によって実行することを特徴とする請求項1 2に記載の通信手段を介したサービス提供方法。

【請求項2 2】前記サービスセンタおよび前記上位機器間のデータ通信は、共通鍵暗号方式によって実行し、前記上位機器および前記制御対象機器間のデータ通信は、共通鍵暗号方式によって実行することを特徴とする請求項1 2に記載の通信手段を介したサービス提供方法。

【請求項2 3】外部ネットワークに対するインターフェース手段と、

暗号処理を実行する暗号処理手段と、ローカルネットワークインターフェース手段または情報記録媒体インターフェース手段とを有し、前記外部ネットワークを介してサービスセンタから受信した制御対象機器に関する暗号化制御情報を前記ローカルネットワークインターフェース手段または情報記録媒体インターフェース手段を介して制御対象機器に転送する構成を有することを特徴とするサービス仲介装置。

【請求項2 4】前記暗号処理手段は前記サービスセンタとの認証処理、前記制御対象機器との認証処理を実行する処理アルゴリズムを格納した構成であることを特徴とする請求項2 3に記載のサービス仲介装置。

【請求項2 5】前記暗号処理手段は、公開鍵暗号方式、共通鍵暗号方式いずれの処理方式にも対応可能な構成を有することを特徴とする請求項2 3に記載のサービス仲介装置。

【請求項2 6】制御対象機器に対する制御情報を通信手段を介して提供するサービス提供処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

サービスセンタから通信手段を介して送信される暗号処理のなされた制御情報を受信するデータ受信ステップと、

受信した暗号化制御情報を、暗号化制御情報としてまたは前記上位機器において復号した復号制御情報としてローカルネットワークインターフェースまたは情報記録媒体を介して前記制御対象機器に転送するデータ転送ステップと、

を有することを特徴とするとするプログラム提供媒体。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】本発明は、通信手段を介したサービス提供システム、サービス提供方法、およびサービス仲介装置に関する。さらに詳細には、各種の電子機

器、例えばテレビやビデオデッキ、エアコン、冷蔵庫、電子レンジなどの各種電子機器に対して、通信ネットワーク等の通信手段を介して各種の制御を実行したり、メンテナンス等のサービスを提供する構成において、個々の機器を小型で低コストの構成とすることを可能とするとともに、サービス提供時の制御情報、メンテナンス情報、課金情報等を十分なセキュリティを確保して転送可能な通信手段を介したサービス提供システム、サービス提供方法、およびサービス仲介装置に関する。

【0002】

【従来の技術】近年、デジタル技術の発展に伴い、多くの電子機器がマイコン等による制御可能な構成となってきている。また複数のコンピュータを結ぶインターネット等の通信ネットワークにより広い地域をカバーするデジタルネットワークが構築されてきている。電子機器を通信ネットワークに接続することによって、電子機器をネットワークを介して遠隔地から制御したりメンテナンスを行なったり、あるいは電子機器ユーザに対してメンテナンス情報の提供を行なうなど、ネットワークを通じた情報伝達形態が盛んになってきている。

【0003】具体的には、各種電子機器に対する制御、メンテナンス等のサービスを提供するサービスセンターを設置し、サービスセンターとユーザの電子機器を電話回線、ケーブルテレビ回線、インターネット、無線回線、衛星回線などで接続して各種サービスを提供する構成が実施されている。また、これらのサービス提供システムにおいてユーザ情報、口座情報等の各種決済情報を登録することにより提供したサービスに対して課金処理を行う構成も普及しつつある。

【0004】

【発明が解決しようとする課題】しかし、このような、電子機器に対するネットワーク等の通信回線を介したサービス提供構成においては、サービス機関とユーザ機器との間をインターネット等の通信手段を介してデータをそのまま送受信することが多いため、例えば個人的な情報が漏洩したり改竄される可能性がある。たとえば、サービス料金に対する課金のためのユーザの銀行口座やクレジットカード番号などの情報は、不正に扱われると重大な被害をもたらす場合があり、インターネットのように複数のユーザが同じ回線を共有するモデルにおいての個人情報を含むデータの送受信は、情報の保護の観点から問題がある。

【0005】また、現在の通信手段を介したサービス提供システムでは、ネットワーク等を介したサービスを受けるために、サービスを受けるすべての機器がサービスセンターと外部ネットワーク等を経由して直接接続できる構成を持つ必要があった。すなわち、サービス通信手段としてのモ뎀、インターフェース等がユーザの機器に備わっていることが必要とされている。しかし、このようなサービスを受けるためにすべての機器に通信のための

モジュールを備えることは、コスト面、機器の小型化の点からも好ましいものではない。特に小型化が重要な機器においてはこの問題は顕著となる。さらに同様の理由で、すべての機器に高度なセキュリティ機能モジュールを構成することも現実的ではなく、これらの問題点がネットワークを介するサービス提供システムの普及を阻む要因の1つとなっている。

【0006】本発明は、上述の問題点、すなわちサービスを受ける電子機器すべてに通信のためのモジュールを備えることを不要とし、また、機器に高度なセキュリティ機能モジュールを構成する必要性をなくすことを可能としたデータ通信システムおよびデータ通信方法を提供することを目的とする。

【0007】

【課題を解決するための手段】本発明の第1の側面は、ローカルネットワークインターフェース手段、または情報記録媒体インターフェース手段の少なくともいずれかを有する前記制御対象機器と、外部ネットワークに対するインターフェース手段と、該外部ネットワークを使用した転送データの暗号処理を実行する暗号処理手段とを有するとともに、前記制御対象機器のローカルネットワークインターフェース手段または情報記録媒体インターフェース手段のいずれかを介して前記制御対象機器に対してデータ転送可能な構成を有する上位機器とを有し、前記上位機器は、前記外部ネットワークを介して前記制御対象機器に対する制御情報をサービスセンターから受信して、該受信制御情報をローカルネットワークまたは情報記録媒体を介して前記制御対象機器に転送する構成を有することを特徴とする通信手段を介したサービス提供システムにある。

【0008】さらに、本発明の通信手段を介したサービス提供システムの一実施態様において、前記サービスセンターおよび前記上位機器は認証処理手段を有し、前記サービスセンターおよび前記上位機器間のデータ送受信は、認証処理による認証が成立した場合にのみ実行する構成であることを特徴とする。

【0009】さらに、本発明の通信手段を介したサービス提供システムの一実施態様において、前記上位機器および前記制御対象機器は認証処理手段を有し、前記上位機器および前記制御対象機器間のデータ送受信は、認証処理による認証が成立した場合にのみ実行する構成であることを特徴とする。

【0010】さらに、本発明の通信手段を介したサービス提供システムの一実施態様において、前記上位機器および前記制御対象機器は認証処理手段を有し、前記上位機器および前記制御対象機器間における前記情報記録媒体の認証処理による認証が成立した場合にのみ実行する構成であることを特徴とする。

【0011】さらに、本発明の通信手段を介したサービス提供システムの一実施態様において、前記サービスセンターは前記上位機器および制御対象機器の機器識別子を登録した機器情報データベースを有し、該機器情報データベースに登録された機器識別子と、前記上位機器または制御対象機器から受信する機器識別子との照合処理を実行することにより、機器正当性検証処理を実行する構成を有することを特徴とする。

【0012】さらに、本発明の通信手段を介したサービス提供システムの一実施態様において、前記サービスセンターは、前記上位機器および制御対象機器の利用者識別子を登録した利用者情報データベースを有し、該利用者情報データベースに登録された利用者識別データと、前記上位機器または制御対象機器から受信する利用者識別データとの照合処理を実行することにより、利用者正当性検証処理を実行する構成を有することを特徴とする。

【0013】さらに、本発明の通信手段を介したサービス提供システムの一実施態様において、前記サービスセンターおよび前記上位機器間ににおいて送受信されるデータは、当該通信セッションでのみ有効なセッション鍵を用いて暗号化処理がなされたデータであることを特徴とする。

【0014】さらに、本発明の通信手段を介したサービス提供システムの一実施態様において、前記上位機器および前記制御対象機器間ににおいて転送されるデータは、当該通信セッションでのみ有効なセッション鍵を用いて暗号化処理がなされたデータであることを特徴とする。

【0015】さらに、本発明の通信手段を介したサービス提供システムの一実施態様において、前記サービスセンターは前記制御対象機器に対して、機器診断処理、機器修復処理、データバックアップ処理、データリストア処理、データ配信処理、ヘルプデータ提供処理、操作情報提供処理のいずれかのサービスを提供する構成であることを特徴とする。

【0016】さらに、本発明の通信手段を介したサービス提供システムの一実施態様において、前記サービスセンターおよび前記上位機器間に認証処理は、公開鍵暗号方式によって実行し、前記上位機器および前記制御対象機器間に認証処理は、公開鍵暗号方式または共通鍵暗号方式によって実行する構成であることを特徴とする。

【0017】さらに、本発明の通信手段を介したサービス提供システムの一実施態様において、前記サービスセンターおよび前記上位機器間のデータ通信は、共通鍵暗号方式によって実行し、前記上位機器および前記制御対象機器間のデータ通信は、共通鍵暗号方式によって実行する構成であることを特徴とする。

【0018】さらに、本発明の第2の側面は、制御対象機器に対する制御情報を通信手段を介して提供するサービス提供方法であり、サービスセンターから、該サービス

センターと通信手段を介して接続される上位機器に対して暗号処理のなされた制御情報を送信するデータ送信ステップと、前記上位機器の受信した暗号化制御情報を、暗号化制御情報としてまたは前記上位機器において復号した復号制御情報としてローカルネットワークインタフェースまたは情報記録媒体を介して前記制御対象機器に転送するデータ転送ステップと、を有することを特徴とするサービス提供方法にある。

【0019】さらに、本発明の通信手段を介したサービス提供方法の一実施態様において、前記サービスセンターから前記上位機器に対するデータ送信ステップの前に、前記サービスセンターと前記上位機器間での認証処理を実行する認証処理ステップを有し、前記データ送信ステップは、前記認証処理ステップにおける認証が成立した場合にのみ実行することを特徴とする。

【0020】さらに、本発明の通信手段を介したサービス提供方法の一実施態様において、前記上位機器から前記制御対象機器に対するデータ転送ステップの前に、前記上位機器と前記制御対象機器間での認証処理を実行する認証処理ステップを有し、前記データ転送ステップは、前記認証処理ステップにおける認証が成立した場合にのみ実行することを特徴とする。

【0021】さらに、本発明の通信手段を介したサービス提供方法の一実施態様において、前記上位機器と前記制御対象機器間でのデータ転送が情報記録媒体を介したデータ転送として行われる場合において、前記上位機器および前記制御対象機器による前記情報記録媒体の認証処理を実行する認証処理ステップを有し、前記データ転送ステップは、前記認証処理ステップにおける認証が成立した場合にのみ実行することを特徴とする。

【0022】さらに、本発明の通信手段を介したサービス提供方法の一実施態様において、前記サービスセンターは前記上位機器および制御対象機器の機器識別子を登録した機器情報データベースを有し、該機器情報データベースに登録された機器識別子と、前記上位機器または制御対象機器から受信する機器識別子との照合処理による機器正当性検証処理ステップを実行することを特徴とする。

【0023】さらに、本発明の通信手段を介したサービス提供方法の一実施態様において、前記サービスセンターは、前記上位機器および制御対象機器の利用者識別子を登録した利用者情報データベースを有し、該利用者情報データベースに登録された利用者識別データと、前記上位機器または制御対象機器から受信する利用者識別データとの照合処理による利用者正当性検証処理ステップを実行することを特徴とする。

【0024】さらに、本発明の通信手段を介したサービス提供方法の一実施態様において、前記サービスセンターまたは前記上位機器のいずれかは、相互に送受信するデータを暗号化する鍵として、当該通信セッションでのみ

有効なセッション鍵を生成し、前記暗号処理は、生成したセッション鍵による暗号化処理として実行することを特徴とする。

【0025】さらに、本発明の通信手段を介したサービス提供方法の一実施態様において、前記上位機器または前記制御対象機器のいずれかは、相互に送受信するデータを暗号化する鍵として、当該通信セッションでのみ有効なセッション鍵を生成し、前記暗号処理は、生成したセッション鍵による暗号化処理として実行することを特徴とする。

【0026】さらに、本発明の通信手段を介したサービス提供方法の一実施態様において、前記サービスセンタは前記制御対象機器に対して、機器診断処理、機器修復処理、データバックアップ処理、データリストア処理、データ配信処理、ヘルプデスク提供処理、操作情報提供処理のいずれかのサービスを提供することを特徴とする。

【0027】さらに、本発明の通信手段を介したサービス提供方法の一実施態様において、前記サービスセンタおよび前記上位機器間の認証処理は、公開鍵暗号方式によって実行し、前記上位機器および前記制御対象機器間の認証処理は、公開鍵暗号方式または共通鍵暗号方式のいずれかの方式によって実行することを特徴とする。

【0028】さらに、本発明の通信手段を介したサービス提供方法の一実施態様において、前記サービスセンタおよび前記上位機器間のデータ通信は、共通鍵暗号方式によって実行し、前記上位機器および前記制御対象機器間のデータ通信は、共通鍵暗号方式によって実行する構成であることを特徴とする。

【0029】さらに、本発明の第3の側面は、外部ネットワークに対するインターフェース手段と、暗号処理を実行する暗号処理手段と、ローカルネットワークインターフェース手段または情報記録媒体インターフェース手段の少なくともいずれかを有し、前記外部ネットワークを介してサービスセンタから受信した制御対象機器に関する暗号化制御情報を前記ローカルネットワークインターフェース手段または情報記録媒体インターフェース手段を介して制御対象機器に転送する構成を有することを特徴とするサービス仲介装置にある。

【0030】さらに、本発明のサービス仲介装置の一実施態様において、前記暗号処理手段は前記サービスセンタとの認証処理、前記制御対象機器との認証処理を実行する処理アルゴリズムを格納した構成であることを特徴とする。

【0031】さらに、本発明のサービス仲介装置の一実施態様において、前記暗号処理手段は、公開鍵暗号方式、共通鍵暗号方式いずれの処理方式にも対応可能な構成を有することを特徴とする。

【0032】さらに、本発明の第4の側面は、制御対象

機器に対する制御情報を通信手段を介して提供するサービス提供処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、サービスセンタから通信手段を介して送信される暗号処理のなされた制御情報を受信するデータ受信ステップと、受信した暗号化制御情報を、暗号化制御情報としてまたは前記上位機器において復号した復号制御情報としてローカルネットワークインターフェースまたは情報記録媒体を介して前記制御対象機器に転送するデータ転送ステップと、を有することを特徴とするとするプログラム提供媒体にある。

【0033】本発明の第4の側面に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、CDやFD、MOなどの記憶媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

【0034】このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働の関係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働の作用が発揮され、本発明の他の側面と同様の作用効果を得ることができる。

【0035】

【作用】本発明の機器およびサービスセンタは相互に認証処理を実行し、通信相手の確認を実行するとともに、送信データの暗号化を行っているため、安全なデータ送受信が可能となる。さらに外部ネットワークに対する通信手段を持たず、サービスセンタに直接接続できない機器も、外部ネットワークと直接接続できる上位機器を介してサービスセンタとの通信を安全に行うことができる。

【0036】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や附する図面に基づくより詳細な説明によって明らかになるであろう。

【0037】

【発明の実施の形態】【システム概要】図1は本発明の通信手段を介したサービス提供システム、サービス提供方法、およびサービス仲介装置の概要を説明するブロック図である。本発明のシステムはユーザー機器に対するサービスを提供するサービスセンタ10、サービスセンタ10とのデータ送受信を実行するサービス仲介装置としての上位機器20、上位機器20を経由して、サービスセンタ10からの制御等を受ける制御対象機器（下位機器）30、サービスセンタ10と上位機器20とを結ぶ

電話回線、CATV回線、衛星、無線、インターネット等の外部ネットワーク通信手段、上位機器20と制御対象機器（下位機器）30との間を結ぶ、例えば、IEEE1394、USB等の通信インターフェースによって通信可能なローカルネットワークからなる。なお、上位機器20自体がサービスセンタ10からの制御、メンテナンス等を受ける制御対象機器となることも可能であり、図1の下側に示す上位機器20は、この態様を示している。

【0038】図1に示した各構成要素について説明する。本発明のユーザ側の機器は上位機器20と制御対象機器（下位機器）30の2種類に大きく分類される。以下、各機器およびサービスセンタの構成について説明する。

【0039】<上位機器>サービス仲介装置としての上位機器20は、サービスセンタ10と電話回線を介した通信が可能なモデム、あるいは、CATV回線、衛星、その他の無線回線等を介したデータ送受信が可能な通信手段を有する機器である。また、図1の上部に示すように、制御対象機器（下位機器）30に対して、サービスセンタ10からのデータを転送したり、制御対象機器（下位機器）30からサービスセンタ10への送信データを転送するための手段を有する。

【0040】図2に上位機器20の構成を示す。上位機器20は、サービスを受ける制御対象機器30との接続用ローカルネットワークを構成するために用いられるIEEE1394（アメリカ電気電子学会による接続規格）やUSB（Universal Serial Bus）等のインターフェース部としてのローカルインターフェース208を備え、他の機器とのデータ通信が可能である。上位機器20とサービスセンタ10との通信は電話回線、ケーブルテレビ回線、無線回線、衛星回線、インターネット接続などによって実行される構成とすればよく、これら各通信方法に従った外部インターフェース206を持つ。

【0041】上位機器20は暗号化・認証や通信の制御を行う専用のICとしての暗号化通信IC205を備える。この暗号化通信IC205は公開鍵暗号方式と共通鍵暗号方式を利用するために必要な演算が可能である。また、ICには上位機器20固有の識別子（機器ID）を格納する記憶手段を備えており、機器の認証の際にこのIDを利用する。暗号化・認証通信IC205は、外部からIDの書き換え等ができないようにSAM（Secure Application Module）として構成されることが好ましい。

【0042】暗号化通信IC205内に格納される機器IDはサービスセンタ10が発行し、サービスセンタのデータベースには発行済みのIDが登録される。なお、セキュリティを高めるために機器IDに、例えば検証ビットを付加する等、冗長性を持たせたデータ構成することにより、サービスセンタ10によるサービス実施時

に機器IDの検証ビットを用いた検証を実行するような構成としてもよい。このような構成とすることにより、サービスセンタ10の発行した正規なID以外の不正なIDを持つ機器をサービス対象から排除することが可能となる。

【0043】公開鍵暗号方式を利用する上で必要となる、上位機器20自身の公開鍵と秘密鍵の組およびその公開鍵に対応する公開鍵証明書は予め機器の暗号化通信IC205の記憶部に記録されている。公開鍵証明書は信頼できる証明書発行機関、いわゆる認証局（CA：Certificate Authority）が発行したものである。

【0044】本発明の通信手段を介したサービス提供システムにおいては、データ送信側とデータ受信側が互いに正規なデータ送受信対象であることを確認した上で、必要な情報を転送する、すなわちセキュリティを考慮したデータ転送構成をとる。データ転送の際のセキュリティ構成を実現する1つの手法が、転送データの暗号化処理である。

【0045】暗号化データは、所定の手続きによる復号化処理によって利用可能な復号データに戻すことができる。暗号化鍵と復号化鍵を用いるデータ暗号化・復号化方法の態様には様々な種類があるが、代表的な例としては暗号化・復号化に共通の鍵を用いるいわゆる公開鍵暗号方式と、暗号化・復号化に異なる鍵を用いる公開鍵暗号方式がある。公開鍵暗号方式は、発信者と受信者の鍵を異なるものとして、一方の鍵を不特定のユーザが使用可能な公開鍵として、他方を秘密に保つ秘密鍵とするものである。例えば、データ暗号化鍵を公開鍵とし、復号鍵を秘密鍵とする。

【0046】暗号化・復号化に共通の鍵を用いるいわゆる共通鍵暗号方式と異なり、公開鍵暗号方式では秘密に保つ必要のある秘密鍵は、特定の1人が持てばよいため鍵の管理において有利である。ただし、公開鍵暗号方式は共通鍵暗号方式に比較してデータ処理速度が遅く、秘密鍵の配送、デジタル署名等のデータ量の少ない対象に多く用いられている。公開鍵暗号方式の代表的なものはRSA（Rivest-Shamir-Adleman）暗号がある。これは非常に大きな2つの素数（例えば150桁）の積を用いるものであり、大きな2つの素数（例えば150桁）の積の素因数分解する処理の困難さを利用してい る。

【0047】公開鍵暗号方式では、不特定多数に公開鍵を使用可能とする構成であり、配布する公開鍵が正当なものであるか否かを証明する証明書、いわゆる公開鍵証明書を使用する方法が多く用いられている。例えば、利用者Aが公開鍵、秘密鍵のペアを生成して、生成した公開鍵を認証局に対して送付して公開鍵証明書を認証局から入手する。利用者Aは公開鍵証明書を一般に公開する。不特定のユーザは公開鍵証明書から所定の手続きを経て公開鍵を入手して文書等を暗号化して利用者Aに送

付する。利用者Aは秘密鍵を用いて暗号化文書等を復号する等のシステムである。

【0048】公開鍵証明書は、公開鍵暗号方式における認証局(CA: Certificate Authority)が発行する証明書であり、ユーザが自己的ID、公開鍵等を認証局に提出することにより、認証局側が認証局のIDや有効期限等の情報を付加し、さらに認証局による署名を付加して作成される証明書である。

【0049】公開鍵証明書は、証明書のバージョン番号、認証局(1A)が証明書利用者に対し割り付ける証明書の通し番号、電子署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、証明書利用者の名前並びに電子署名を含む。

【0050】電子署名は、証明書のバージョン番号、認証局が証明書利用者に対し割り付ける証明書の通し番号、電子署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、証明書利用者の名前並びに証明書利用者の公開鍵等の全体データに対しハッシュ関数を適用してハッシュ値を生成し、そのハッシュ値に対して認証局の秘密鍵を用いて生成したデータである。

【0051】認証局は、公開鍵証明書を発行とともに、有効期限が切れた公開鍵証明書を更新し、不正を行った利用者の排斥を行うための不正者リストの作成、管理、配布(これをリボケーション:Revocationと呼ぶ)等の処理を行う。

【0052】一方、この公開鍵証明書を利用する際には、利用者は自己が保持する認証局の公開鍵を用い、当該公開鍵証明書の電子署名を検証し、電子署名の検証に成功した後に公開鍵証明書から公開鍵を取り出し、当該公開鍵を利用する。従って、公開鍵証明書を利用する全ての利用者は、共通の認証局の公開鍵を保持している必要がある。本発明の図2に示す上位機器20では、認証局の公開鍵は暗号化通信IC205の内部メモリに格納されている。

【0053】なお、上位機器の公開鍵、秘密鍵は、サービスセンタ10に対して機器登録を実行する際に新たに上位機器が生成、あるいはサービスセンタが生成してこれを受信して上位機器に格納する構成としてもよく、この場合、公開鍵証明書が必要であれば、別途認証局から取得する。

【0054】また、上位機器20は、複数の鍵の組が格納可能であり、機器が接続するサービスセンタ毎もしくはサービス毎に鍵の組を変更することができる。上位機器20には、様々な下位機器としての制御対象機器30がローカル接続可能であり、例えば制御対象機器30がAメーカーのテレビであれば、Aメーカーのサービスセンタ接続用の鍵を用い、制御対象機器30がBメーカーのエアコンであれば、Bメーカーのサービスセンタ接続用の

鍵を用いる等の構成が可能となる。

【0055】上位機器20は、さらに、暗号化通信IC205の処理制御、各インターフェースを介した通信制御、記憶装置210のデータアクセス制御等の各種処理を制御するためのCPU201、通信データの一時記憶、処理プログラムの格納部として機能するRAM、ROM等によって構成されるメモリ202、機器を操作するユーザーに対する指示データ等の表示を行なう表示部203、ユーザーによる通信開始等の指示を可能とする操作部209、ハードディスク、CD、DVD等によって構成される記憶装置210を備える。

【0056】さらに上位機器20は、機器本来の機能を提供する機器固有部204を有する。機器固有部204は、機器がたとえビデオデッキであれば受信データの処理回路や変調回路、あるいは磁気ドラムやテープ駆動部等であり、例えば電子レンジ等であれば、電子レンジの処理機能を含む。さらに上位機器20は、メモリースティック、FD、CD、DVDのような情報記録媒体211にデータを記録するように構成してもよい。その場合、情報記録媒体211とのインターフェース207を備える。

【0057】<制御対象機器(下位機器)>制御対象機器(下位機器)30は、外部ネットワークとの直接接続手段を持たない機器であり、上位機器20にローカルネットワークを介して接続され、サービスセンタ10からの制御、メンテナンス等各種サービスを受ける機器である。

【0058】図3、図4に制御対象機器(下位機器)30の2つの構成例を示す。図3は、制御対象機器(下位機器)30が、上位機器と接続するためのローカルネットワークインターフェース307を有する構成であり、このローカルネットワークインターフェース307を介して上位機器20と接続され、上位機器20を介して受信するサービスセンタ10の制御を受ける。この態様をオンライン型下位機器と呼ぶ。

【0059】一方、図4に示す制御対象機器(下位機器)30は、上位機器と接続するためのローカルネットワークインターフェースを持たない構成であり、メモリカード、CD、FD等の情報記録媒体310に格納された制御情報、メンテナンス情報に基づいて制御を受ける。サービスセンタ10から受信した制御情報を前述の図2の上位機器の情報記録媒体211に格納し、これを制御対象機器(下位機器)30に取り付けることによってサービスセンタ10からの制御をオフライン制御として実行することを可能としたものである。

【0060】制御対象機器(下位機器)30の構成について説明する。図3のオンライン型の場合、サービスを受ける制御対象機器(下位機器)30は、上位機器20との接続用ローカルネットワークを構成するためIEEE1394やUSB(Universal Serial Bus)等のインタ

一フェース部としてのローカルインターフェース 307 を備え、上位機器 20 とのデータ通信が可能である。

【0061】制御対象機器（下位機器）30 は暗号化・認証や通信の制御を行う専用の I C としての暗号化通信 I C 305 を備える。この暗号化通信 I C 305 は公開鍵暗号方式と共通鍵暗号方式を利用するために必要な演算が可能である。また、暗号化通信 I C 305 は公開鍵暗号方式と共通鍵暗号方式を利用するために必要な演算が可能である。ただし公開鍵暗号方式を利用するには高い演算能力が必要であることから、資源に制約のある機器においては共通鍵暗号方式のみを利用可能とする構成としてもよい。

【0062】公開鍵暗号方式を利用する上で必要となる、公開鍵と秘密鍵の組およびその公開鍵に応じる公開鍵証明書は予め制御対象機器（下位機器）30 の暗号化通信 I C 305 の内部メモリに記録されている。公開鍵証明書は上述した上位機器 20 の場合と同様、信頼できる証明書発行機関、いわゆる認証局（C A : Certificate Authority）が発行したものである。なお、制御対象機器（下位機器）30 の公開鍵、秘密鍵は、サービスセンタ 10 に対して機器登録を実行する際に新たに生成、あるいはサービスセンタが生成してこれを受信して機器に格納する構成としてもよく、この場合、公開鍵証明書が必要であれば、別途認証局から取得する。また、制御対象機器（下位機器）30 は、複数の鍵の組を格納可能とした構成としてもよく、機器が接続するサービスセンタ毎もしくはサービス毎に鍵の組を変更することを可能とした構成としてもよい。なお、サービスセンタ 10 の公開鍵は予め機器の暗号化通信 I C 305 の内部メモリに記録されている。なお、共通鍵暗号方式のみを利用する構成とする場合には、共通鍵はサービスセンタ 10 によって発行され、制御対象機器（下位機器）30 の暗号化通信 I C 305 の内部メモリに格納する。なお、共通鍵は制御対象機器（下位機器）30 の識別子（I D）に対応してサービスセンタが保持してもよい。

【0063】制御対象機器（下位機器）30 は、さらに、暗号化通信 I C 305 の処理制御、各インターフェースを介した通信制御、記憶装置 309 のデータアクセス制御等の各種処理を制御するための C P U 301、通信データの一時記憶、処理プログラムの格納部として機能する R A M 、 R O M 等によって構成されるメモリ 302、機器を操作するユーザに対する指示データ等の表示を行なう表示部 303、ユーザによる通信開始等の指示を可能とする操作部 308、ハードディスク、 C D 、 D V D 等によって構成される記憶装置 309 を備える。

【0064】さらに制御対象機器（下位機器）30 は、機器本来の機能を提供する機器固有部 304 を有する。さらに制御対象機器（下位機器）30 は、メモリーステイック、 F D 、 C D 、 D V D のような情報記録媒体 310 にデータを記録するように構成してもよい。その場

合、情報記録媒体 310 とのインターフェース 306 を備える。図 4 のオフライン型の場合、この情報記録媒体 310 を介してサービスセンタ 10 からの制御情報を受領する。図 3 のオンライン型構成では、ローカルネットワークを介するか、あるいは情報記録媒体 310 を介するか、いずれの方法も可能となる。

【0065】すなわち、図 3 のオンライン型では、制御対象機器（下位機器）30 はサービスを受ける際、ローカルネットワークインターフェース 307 を用いて上位機器 20 に接続し、上位機器 20 の外部インターフェース 206 の接続能力を利用してサービスセンタ 10 と接続する。このとき通信制御は制御対象機器（下位機器）30 が独自に行う。また、図 4 のオフライン型では、上位機器 20 が制御対象機器（下位機器）30 の代理としてセンタに接続してデータを送受信し、制御対象機器（下位機器）30 はそのデータを上位機器 20 で情報記録媒体に記録し、その情報記録媒体を制御対象機器（下位機器）30 に移動し、制御対象機器（下位機器）30 はその情報記録媒体からデータを読み出す。

【0066】なお、上述した図 3 のオンライン型、図 4 のオフライン型の制御対象機器（下位機器）30 は、暗号化通信 I C 305 を有しており、暗号化処理の可能な構成として説明したが、下位機器においては暗号化を行なわず通信を制御する I C だけを備えた構成としてもよく、この場合は通信回線を介してオンライン接続、または記憶媒体を介してオフライン接続した上位機器が通信内容の暗号化処理を代行することが可能である。この場合の制御対象機器（下位機器）30 と上位機器 20 との認証には機器識別子（I D）による認証を実行する。

【0067】<サービスセンタ>サービスセンタ 10 の構成例を図 5 に示す。サービスセンタ 10 は、外部ネットワークインターフェース 105 および暗号化通信 I C 104 、サービス提供用データベース 103 、機器情報データベース 106 、利用者情報データベース 107 、 C P U 101 、メモリ 102 、さらにつなぐ接続するデータベースで構成される。

【0068】暗号化通信 I C 104 は上位機器 20 との通信およびデータの暗号化、サービス提供対象機器の認証などの処理を行う。この暗号化通信 I C 104 にはサービスセンタ固有のセンタ識別子（I D）が記録されており、これは通信相手となる各機器との相互認証の際に利用する。

【0069】サービスセンタ 10 の暗号化通信 I C 104 は公開鍵暗号方式および共通鍵暗号方式を利用するために必要な演算が可能である。機器情報データベース 106 には、通信対象、たまにサービス対象各機器の識別子（I D）や公開鍵などの情報が格納されている。データ通信において共通鍵暗号方式を利用する機器の場合には、あらかじめ機器 I D とそれに対応する共通鍵をこの機器情報データベース 106 に格納しておく。

【0070】利用者情報データベース107には、サービスセンタ10からのサービスの提供を受ける機器を管理し、サービスの対応等の支払処理を行なうユーザ、すなわちサービス利用者の識別子（ID）や各利用者の決済情報などが格納されている。サービス提供用データベース103には、サービスを提供するために必要なデータが格納されている。CPU101は、暗号化通信IC104の処理制御、各インターフェースを介した通信制御、各記憶装置のデータアクセス制御等の各種処理を制御を行ない、メモリ102は、通信データの一時記憶、処理プログラムの格納部として機能するRAM、ROM等によって構成される。

【0071】【暗号化・認証レベル】本発明の通信手段を介したサービス提供システムにおいて用いられる公開鍵暗号方式としてはRSA等、また共通鍵暗号方式としてはDES等の暗号方式を用いることが可能であり、必要な強度等を勘案して適切な方式を用いて良い。

【0072】図6は本発明におけるサービスセンタ10と上位機器20、制御対象機器（下位機器）30との間の接続形態と暗号化・認証レベルをまとめたものである。

【0073】サービスセンタ10と上位機器20とは外部ネットワークで接続されている。また暗号化・認証は公開鍵暗号方式を利用。上位機器20と制御対象機器（下位機器）30との接続の形態には6種類ある。すなわち、（1）制御対象機器（下位機器）30がローカルネットワークに接続可能で公開鍵暗号方式が利用できる場合、（2）制御対象機器（下位機器）30がローカルネットワークに接続可能で暗号が利用できない場合、（3）制御対象機器（下位機器）30が記録媒体の移動によりデータ交換可能で公開鍵暗号方式が利用できる場合、（4）制御対象機器（下位機器）30が記録媒体の移動によりデータ交換可能で暗号が利用できない場合、（5）制御対象機器（下位機器）30が記録媒体の移動によりデータ交換可能で共通鍵暗号方式のみが利用できる場合、（6）制御対象機器（下位機器）30が記録媒体の移動によりデータ交換可能で暗号が利用できない場合である。なお、一台の上位機器には複数の下位機器を接続可能であり、上位機器20は、複数の暗号方式に対応可能な構成することにより、様々なタイプの制御対象機器（下位機器）との通信が可能となる。なお、制御対象機器（下位機器）の機器IDを参照することにより、上位機器は配下の下位機器を識別可能である。

【0074】【全体フロー】本発明の通信手段を介したサービス提供システムにおける上位機器20および制御対象機器（下位機器）30のサービスセンタ10を利用した遠隔サービスの提供処理について、以下説明する。

【0075】図7から図10までの図はサービス開始から終了に至るまでの全体の処理の流れを簡潔に示したフ

ロー図である。これらのフロー中に含まれる処理の詳細については、後段で説明する。まず、図7～10を用いて本発明のサービス提供システムの処理の流れの概要を説明する。

【0076】まず、図7のフローに示すように、上位機器20をネットワークを介してサービスセンタ10に対して初めて接続する場合には、ステップS701に示すサービスセンタ10への機器登録を行う。初接続時の処理が終了している場合、もしくは機器登録が不要な処理、例えばフリーメンテナンス提供等の場合には、ステップS702に示す機器認証のステップに移る。機器認証処理フローを図7に示す。これは上位機器20およびサービスセンタ10が相互に通信相手の正当性を確認する手続きである。図に示す機器登録プロトコル、機器認証プロトコルについては後段で詳細に説明する。

【0077】図7に示す、認証プロトコルを実行することにより、不正な機器がサービスを受けたり、サービスセンタ10と誤って通信を行うことを防ぐことができる。ステップS702の機器認証に失敗した場合には、エラー処理を行った後、処理を中止する。機器認証に成功した場合は、必要なならば利用者登録を行う。

【0078】図8に示す利用者登録手続きでは、サービスセンタ10の利用者情報データベース（図5に示す107）に、機器の利用者情報、例えば氏名、サービス料金決済用のクレジットカード番号、あるいは銀行口座番号等の必要情報を登録（ステップS801）する。その後パスワード等の利用者認証に必要な情報登録（ステップS802）も行う。

【0079】図9は、上段が利用者情報、例えば氏名、クレジット番号等の利用者情報変更手続きを示す処理であり、下段が、パスワード等の利用者認証に必要な情報の変更手続きを示すフローである。利用者情報変更手続きでは最初に利用者認証（ステップS901）を行う。これは正当な利用者以外の者が不正に他人の利用者情報を変更することを防ぐためである。利用者認証に失敗した場合には、エラー処理を行った後、処理を中止する。利用者認証に成功した場合は、続いて利用者情報登録（ステップS902）を行う。

【0080】利用者情報の登録が完了すると、必要な場合に限り利用者認証に必要な情報、例えばパスワード等の利用者認証情報変更手続きを行う。利用者認証情報変更手続きでは、最初に利用者認証を行う。これは正当な利用者以外の者が不正に他人のパスワード等の利用者認証情報を変更することを防ぐためである。利用者認証に失敗した場合には、エラー処理を行った後、処理を中止する。利用者認証に成功した場合は、続いて利用者認証情報の変更（ステップS903）を行う。以上の手続きが終了し、サービスを実施する場合にはサービス実施手続きを行う。

【0081】図10に制御対象機器の制御、メンテナン

ス等のサービスの実行処理、すなわちサービス実施手続きフローを示す。サービス実施手続きでは、必要であれば最初に利用者認証を行う。これは正当な利用者以外の者が不正にサービスを受けることを防ぐためである。利用者認証を行なうかどうかは、サービスによって異なる。利用者認証に失敗した場合には、エラー処理を行なった後、処理を中止する。利用者認証に成功した場合は、統いてサービスを行う。サービスが完了した後、接続を終了しない場合は機器認証終了時以降の手続きを再度行う。

【0082】 [各プロトコルについて]

（1）機器登録プロトコル

a. 上位機器

まず、上位機器 2 0 をサービスセンタ 1 0 に対して登録するプロトコルについて説明する。このプロトコルは機器 ID、機種名、機器公開鍵をセンタの機器情報データベースに登録するためのプロトコルである。

【0083】先の図 6 で説明したように上位機器 2 0 とサービスセンタ 1 0 の間では、公開鍵暗号方式によって相互認証、データ通信が実行される。公開鍵暗号方式を利用する上で必要となる、上位機器自身の公開鍵と秘密鍵の組があらかじめ上位機器 2 0 の暗号化通信 I C 2 0 5 の内部メモリに格納されている場合と、これらの鍵を暗号化通信 I C 2 0 5 の内部メモリにあらかじめ格納せず、サービスセンタ 1 0 との接続が必要になった時点でのサービスセンタ 1 0 に機器登録を行い、その際にそれぞれの鍵を生成する構成の 2 つの構成がある。前者の鍵格納済みの場合のプロトコルを図 1 1 に示し、鍵を生成する場合のプロトコルを図 1 2 に示す。

【0084】図 1 1、図 1 2 の処理について説明する。機器登録を行う場合、上位機器 2 0 はサービスセンタ 1 0 に機器登録開始要求を送信する。サービスセンタ 1 0 は要求に応えられる状態であれば、機器登録開始可能であることを機器に通知する。同時にサービスセンタ 1 0 は自身のセンタ識別子（ID）を送信する。

【0085】上位機器 2 0 はサービスセンタ 1 0 から送られてきたサービスセンタ識別子（ID）によりセンタを確認し、サービスセンタ 1 0 に自身の上位機器識別子（ID）、機種名および公開鍵証明書を送信する。上位機器 2 0 の暗号化通信 I C 2 0 5 にはサービスセンタ 1 0 の公開鍵が格納されており、サービスセンタ 1 0 への送信の際にはこの公開鍵を用いて送信データを暗号化する。

【0086】なお、図 1 2 に示す例のように、上位機器 2 0 自身が鍵の組を生成する場合には公開鍵証明書のかわりに上位機器 2 0 が生成した公開鍵をセンタに送信する。

【0087】上位機器 2 0 からサービスセンタ 1 0 への送信データは、サービスセンタ 1 0 の公開鍵で暗号化されているので、送信データに含まれる上位機器識別子

（ID）、機種名等のデータが第三者に漏洩したり、改竄されたりする可能性を排除できる。

【0088】上位機器識別子（ID）等のデータを愛信したセンタは、サービスセンタ 1 0 自身の秘密鍵で上位機器から送られてきたデータを復号する。復号したデータ中の上位機器識別子（ID）の検証を行い、正当な識別子（ID）であれば、送信データ中の上位機器識別子（ID）、機種名および公開鍵証明書もしくは公開鍵を機器情報データベース 1 0 6 に登録する。データベースへの登録が正常に終了した場合には、サービスセンタ 1 0 は上位機器 2 0 に機器登録処理完了通知を返す。データの復号あるいは上位機器識別子（ID）の正当性検証、データベースへの登録が失敗した場合には、サービスセンタ 1 0 は上位機器 2 0 にエラー通知を返す。

【0089】 b. 制御対象機器（下位機器）

次に、制御対象機器（下位機器） 3 0 をサービスセンタ 1 0 に対して登録するプロトコルについて説明する。

【0090】制御対象機器（下位機器） 3 0 が機器登録を行う場合には、オンライン型下位機器とオフライン型下位機器で手順が異なる。さらに公開鍵暗号方式が利用できる機器とできない機器とでも異なる。なお、制御対象機器（下位機器） 3 0 が接続する上位機器 2 0 は、この手順を以て前に上位機器 2 0 とサービスセンタ 1 0 間での機器認証プロトコルを実施しており、センタとの間で認証がなされているものとする。

【0091】 b-1. 公開鍵暗号方式のオンライン型下位機器

最初にオンライン型下位機器を用いる場合の手順について図 1 3 に示す。オンライン型下位機器で公開鍵が利用できる場合、公開鍵暗号方式を利用することによって必要となる、制御対象機器（下位機器） 3 0 自身の公開鍵と秘密鍵の組があらかじめ制御対象機器（下位機器） 3 0 の暗号化通信 I C 3 0 5 の内部メモリに格納されている場合と、これらの鍵を暗号化通信 I C 3 0 5 の内部メモリに格納せず、サービスセンタ 1 0 との接続が必要になった時点でのサービスセンタ 1 0 に機器登録を行い、その際にそれぞれの鍵を生成する構成の 2 つの構成がある。前者の鍵格納済みの場合のプロトコルを図 1 3 に示し、鍵を生成する場合のプロトコルを図 1 4 に示す。

【0092】図 1 3、図 1 4 の処理について説明する。機器登録を行う場合、最初に制御対象機器（下位機器） 3 0 は上位機器 2 0 に対して機器登録開始要求を発行する。これを受け取った上位機器 2 0 はサービスセンタ 1 0 に機器登録開始要求を中継する。サービスセンタ 1 0 は要求に応えられる状態であれば、機器登録開始可能であることを上位機器 2 0 に通知する。そして上位機器 2 0 は機器登録開始が可能であることを制御対象機器（下位機器） 3 0 に対して通知する。

【0093】この機器登録開始確認通知を受け取ると、制御対象機器（下位機器） 3 0 は制御対象機器（下位機

器）自身の機器ID、機種名、公開鍵証明書をセンタの公開鍵で暗号化し、上位機器に送信する。なお、図14に示すように下位機器が鍵の組を生成する場合には、公開鍵証明書の代わりに自身の公開鍵を上位機器20に送信する。これを受け取った上位機器20は、これらの受信データをそのままサービスセンタに中繼する。

【0094】制御対象機器（下位機器）30から上位機器20、サービスセンタ10へ送信されるデータは、サービスセンタ10の公開鍵で暗号化されているので、送信データに含まれる制御対象機器（下位機器）識別子（ID）、機種名等のデータが第三者に漏洩したり、改竄されたりする可能性を排除できる。

【0095】制御対象機器（下位機器）識別子（ID）等のデータを受信したセンタは、サービスセンタ10自身の秘密鍵で上位機器から送られてきたデータを復号する。復号したデータ中の制御対象機器（下位機器）識別子（ID）の検証を行い、正当な識別子（ID）であれば、送信データ中の制御対象機器（下位機器）識別子（ID）、機種名および公開鍵証明書もしくは公開鍵を機器情報データベース106に登録する。データベースへの登録が正常に終了した場合には、サービスセンタ10は上位機器20に機器登録処理完了通知を返す。データの復号あるいは上位機器識別子（ID）の正当性検証、データベースへの登録が失敗した場合には、サービスセンタ10は上位機器20にエラー通知を返す。

【0096】上位機器20はサービスセンタ10から受信した処理完了通知もしくはエラー通知を制御対象機器（下位機器）30に中繼する。

【0097】b-2. 共通鍵暗号方式のオンライン型下位機器

公開鍵暗号方式が利用できず、共通鍵方式が利用可能もしくは暗号化機能がないオンライン型下位機器の機器登録手順について述べる。

【0098】この場合のプロトコルを図15に示す。この場合も、上位機器20は機器登録開始が可能であることを制御対象機器（下位機器）30に対して通知するまでの処理は同一である。制御対象機器（下位機器）30が機器登録開始確認通知を受け取ると、制御対象機器（下位機器）30は自身の機器ID、機種名を上位機器20に送信する。

【0099】この場合、上位機器20に送信される機器ID、機種名情報は暗号化されていないが、ローカルネットワーク上であるので外部ネットワークに比べてセキュリティ上の問題は比較的少ないと考えられる。上位機器20は制御対象機器（下位機器）30から受け取った情報をサービスセンタ10の公開鍵で暗号化する。すなわち、上位機器20がデータの暗号化を代行する。この後の処理は公開鍵暗号方式が利用できる下位機器の場合の手順と同一であるので説明を省略する。

【0100】b-3. 公開鍵暗号方式のオフライン型下

位機器

続いてオフライン型下位機器における機器登録手順について述べる。オフライン型下位機器で公開鍵暗号方式が利用できる場合、公開鍵暗号方式を利用する上で必要となる、制御対象機器（下位機器）30自身の公開鍵と秘密鍵の組があらかじめ制御対象機器（下位機器）30の暗号化通信IC305の内部メモリに格納されている場合と、これらの鍵を暗号化通信IC305の内部メモリに格納せず、サービスセンタ10との接続が必要になった時点でのサービスセンタ10に機器登録を行い、その際にそれぞれの鍵を生成する構成の2つの構成がある。前者の鍵格納済みの場合のプロトコルを図16に示し、鍵を生成する場合のプロトコルを図17に示す。

【0101】図16、図17の処理について説明する。制御対象機器（下位機器）30は最初に情報記録媒体を認証する。情報記録媒体310は例えばメモリカードであれば、メモリカードの識別子等を用いた認証処理が実行される。認証が成功すると、制御対象機器（下位機器）30は自身の制御対象機器（下位機器）識別子（ID）、機種名および公開鍵証明書（図16）もしくは公開鍵（図17）をサービスセンタの公開鍵で暗号化し、情報記録媒体310に転送する。

【0102】データ転送が完了した後、情報記録媒体310を制御対象機器（下位機器）30の下位機器から取り外し、上位機器20に装着する。上位機器20は情報記録媒体211（情報記録媒体310と同じ）が装着されると、情報記録媒体の認証を開始する。情報記録媒体認証が終了した後、上位機器20は情報記録媒体からデータを転送（読み出し処理）する。転送終了後、上位機器20はサービスセンタ10に機器登録開始要求を制御対象機器（下位機器）30の代理として行う。

【0103】サービスセンタ10は要求に応えられる状態であれば、機器登録開始可能であることを上位機器20に通知する。そして上位機器20は情報記録媒体211から転送したデータをそのままセンタに送信する。情報記録媒体211から読み出された制御対象機器（下位機器）識別子（ID）等のデータを受信したセンタは、自身の秘密鍵で上位機器20が中継したデータを復号する。その後復号したデータ中の制御対象機器（下位機器）識別子（ID）の検証を行い、正当なIDであれば、受信した制御対象機器（下位機器）識別子（ID）、機種名および公開鍵証明書（図16）もしくは公開鍵（図17）を機器情報データベース106に登録する。データベースへの登録が正常に終了した場合には、サービスセンタ10は上位機器20に処理完了通知を返す。データの復号あるいは制御対象機器（下位機器）識別子（ID）の正当性検証、データベースへの登録が失敗した場合には、サービスセンタ10は上位機器20にエラー通知を返す。上位機器20は情報記録媒体211に処理完了通知もしくはエラー通知を転送する。その

後、情報記録媒体 2 1 1 を上位機器 2 0 から制御対象機器（下位機器）3 0 に移動する。制御対象機器（下位機器）3 0 は情報記録媒体認証を行った後、サービスセンタ 1 0 からの通知を情報記録媒体から転送する。通知内容がエラー通知であれば、再度機器登録を試みる。

【0 1 0 4】b - 4. 共通鍵暗号方式のオフライン型下位機器

公開鍵暗号方式が利用できず、共通鍵方式が利用可能もしくは暗号化機能がないオフライン型下位機器の機器登録手順について述べる。この場合のプロトコルを図 1 8 に示す。制御対象機器（下位機器）3 0 は最初に情報記録媒体 3 1 0 を認証する。その後、制御対象機器（下位機器）3 0 は自身の機器 ID、機種名を情報記録媒体 3 1 0 に転送する。転送が完了した後、情報記録媒体 3 1 0 を制御対象機器（下位機器）3 0 から取り外し、上位機器 2 0 に装着する。

【0 1 0 5】上位機器 2 0 は情報記録媒体 2 1 1 (=情報記録媒体 3 1 0) が装着されると、情報記録媒体 2 1 1 の認証を開始する。情報記録媒体 2 1 1 の認証が終了した後、上位機器 2 0 は情報記録媒体 2 1 1 からデータを転送する。転送終了後、上位機器 2 0 はサービスセンタ 1 0 に機器登録開始要求を送信する。サービスセンタ 1 0 は要求に応える状態であれば、機器登録開始可能であることを上位機器 2 0 に通知する。上位機器 2 0 は情報記録媒体 2 1 1 から転送したデータをサービスセンタ 1 0 の公開鍵で暗号化し、センタに送信する。情報記録媒体 2 1 1 から読み出された制御対象機器（下位機器）識別子（ID）等のデータを受信したセンタは、自身の秘密鍵で上位機器 2 0 が中継したデータを復号する。その後復号したデータ中の制御対象機器（下位機器）識別子（ID）の検証を行い、正当な ID であれば、受信した制御対象機器（下位機器）識別子（ID）、機種名を機器情報データベース 1 0 6 に登録する。その後の処理完了通知などの処理は、公開鍵暗号方式が利用できるオフライン型下位機器を用いる場合と同様である。

【0 1 0 6】【機器認証プロトコル】次に、サービスセンタ 1 0 、上位機器 2 0 、制御対象機器（下位機器）3 0 の相互において実行される機器認証プロトコルの詳細について説明する。機器認証プロトコルは、データ通信を行なう 2 者間で通信相手の正当性を確認するために実行されるプロセスである。相互認証処理時にセッション鍵の生成を実行して、生成したセッション鍵を共有鍵として暗号化処理を実行してデータ送信を行なう構成が 1 つの好いデータ転送方式である。以下、上位機器 2 0 を中心として行われる機器認証プロトコルと、制御対象機器（下位機器）3 0 を中心として行われる機器認証プロトコルについて、それぞれ説明する。

【0 1 0 7】a. 上位機器
まず、上位機器 2 0 とサービスセンタ 1 0 の間で実行

される互いの正当性を確認する機器認証プロトコルについて説明する。

【0 1 0 8】図 1 9 にサービスセンタ 1 0 と上位機器 2 0 が機器認証を行う場合のプロトコルを示す。まず上位機器 2 0 はサービスセンタ 1 0 に機器認証開始要求を送信する。サービスセンタ 1 0 は要求に応えられる状態であれば、機器認証開始可能であることを機器に通知する。この際、サービスセンタ 1 0 は自身のセンタ ID を送信する。

【0 1 0 9】上位機器 2 0 はサービスセンタ 1 0 から、認証開始可能の応答を受領すると、上位機器 2 0 自身の機器 ID を送信する。その後、サービスセンタ 1 0 と上位機器 2 0 の間に相互認証を行う。相互認証の手続きとしては、たとえば ISO 9 7 9 8 に示されている手続きを利用することができる。

【0 1 1 0】ISO 9 7 9 8 の相互認証手続きとして、公開鍵暗号方式である 1 6 0 ビット長の楕円曲線暗号を用いた相互認証方法を、図 2 0 を用いて説明する。図 2 0 において、公開鍵暗号方式として ECC を用いているが、同様な公開鍵暗号方式であればいずれでもよい。また、鍵サイズも 1 6 0 ビットでなくてもよい。図 2 0 において、A、B の一方がサービスセンタ 1 0 、他方が上位機器 2 0 に相当する。

【0 1 1 1】まず B が、6 4 ビットの乱数 R_b を生成し、A に送信する。これを受信した A は、新たに 6 4 ビットの乱数 R_a および標数 p より小さい乱数 A_k を生成する。そして、ベースポイント G を B_k 倍した点 A_v = A_k × G を求め、R_a、R_b、A_v (X 座標と Y 座標) に対する電子署名 A_sig を生成し、A の公開鍵証明書とともに B に返送する。ここで、R_a および R_b はそれぞれ 6 4 ビット、A_v の X 座標と Y 座標がそれぞれ 1 6 0 ビットであるので、合計 4 4 8 ビットに対する電子署名を生成する。

【0 1 1 2】公開鍵証明書を利用する際には、利用者は自己が保持する公開鍵証明書認証局 (CA) の公開鍵を用い、当該公開鍵証明書の電子署名を検証し、電子署名の検証に成功した後に公開鍵証明書から公開鍵を取り出す。

【0 1 1 3】A の公開鍵証明書、R_a、R_b、A_v、電子署名 A_sig を受信した B は、A が送信してきた R_b が、B が生成したものと一致するか検証する。その結果、一致していた場合には、A の公開鍵証明書内の電子署名を認証局の公開鍵で検証し、A の公開鍵を取り出す。そして、取り出した A の公開鍵を用い電子署名 A_sig を検証する。電子署名の検証に成功した後、B は A を正当なものとして認証する。

【0 1 1 4】次に、B は、標数 p より小さい乱数 B_k を生成する。そして、ベースポイント G を B_k 倍した点 B_v = B_k × G を求め、R_b、R_a、B_v (X 座標と Y 座標) に対する電子署名 B_sig を生成し、B の公開鍵

証明書とともにAに返送する。

【0115】Bの公開鍵証明書、R_b、R_a、A_v、電子署名B、S_{ig}を受信したAは、Bが送信してきたR_aが、Aが生成したものと一致するか検証する。その結果、一致していた場合には、Bの公開鍵証明書内の電子署名を認証局の公開鍵で検証し、Bの公開鍵を取り出す。そして、取り出したBの公開鍵を用い電子署名B、S_{ig}を検証する。電子署名の検証に成功した後、AはBを正当なものとして認証する。

【0116】両者が認証に成功した場合には、BはB_k×A_v（B_kは乱数だが、A_vは椭円曲線上の点であるため、椭円曲線上の点のスカラーベ倍計算が必要）を計算し、AはA_k×B_vを計算し、これら点のX座標の下位64ビットをセッション鍵として以降の通信に使用する（共通鍵暗号を64ビット鍵長の共通鍵暗号とした場合）。もちろん、Y座標からセッション鍵を生成してもよいし、下位64ビットでなくともよい。なお、相互認証後の秘密通信においては、送信データはセッション鍵で暗号化されるだけでなく、電子署名も付されることがある。

【0117】電子署名の検証や受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

【0118】このような相互認証処理において生成したセッション鍵を用いて、送信データを暗号化して、相互にデータ通信を実行することにより、第三者に対する通信データの漏洩が防止される。なお、データの暗号化に必要なセッション鍵の生成はサービスセンタ10、上位機器20のどちらが行ってもよい。相互認証やセッション鍵の交換が失敗した場合には、サービスセンタ10は上位機器20にエラーを返す。すべての処理が完了したならば、センタは上位機器に処理完了を通知する。

【0119】b-1. オンライン型下位機器
次にサービスセンタ10とオンライン型の制御対象機器（下位機器）30とが機器認証を行う場合について述べる。この場合のプロトコルを図21に示す。

【0120】まずオンライン型の制御対象機器（下位機器）30は上位機器20に機器認証開始要求を送信する。上位機器20は要求に応えられる状態であれば、機器認証開始可能であることを制御対象機器（下位機器）30に通知する。制御対象機器（下位機器）30は上位機器20に自身の機器IDを送信する。そして上位機器20と制御対象機器（下位機器）30との間で相互認証を行う。

【0121】なお、上位機器20と制御対象機器（下位機器）30との間での相互認証は、前述のサービスセンタ10と上位機器20との間の相互認証処理として説明した図20の公開鍵暗号方式の認証処理として行なってよいし、共通鍵暗号方式による相互認証を行なってよい。

【0122】共通鍵暗号方式を用いた相互認証方法を、図22を用いて説明する。図22は共通鍵暗号方式としてDESを用いた例であるが、同様な共通鍵暗号方式であればその他の方法も適用可能である。図22において、A、Bのいずれかが上位機器20、他方が制御対象機器（下位機器）30に対応する。

【0123】まず、Bが64ビットの乱数R_bを生成し、R_bおよび自己のIDであるID（b）をAに送信する。これを受信したAは、新たに64ビットの乱数R_aを生成し、R_a、R_b、ID（b）の順に、DESのCBCモードで鍵K_aを用いてデータを暗号化し、Bに返送する。

【0124】これを受信したBは、受信データを鍵K_aで復号化する。受信データの復号化方法は、まず、暗号文E1を鍵K_aで復号化し、乱数R_aを得る。次に、暗号文E2を鍵K_aで復号化し、その結果とE1を掛ける論理和し、R_bを得る。最後に、暗号文E3を鍵K_aで復号化し、その結果とE2を掛ける論理和し、ID（b）を得る。こうして得られたR_a、R_b、ID（b）の内、R_bおよびID（b）が、Bが送信したものと一致するか検証する。この検証に通った場合、BはAを正当なものとして認証する。

【0125】次にBは、認証後に使用するセッション鍵(Session Key(以下、K_{ses}とする))を生成する（生成方法は、乱数を用いる）。そして、R_b、R_a、K_{ses}の順に、DESのCBCモードで鍵K_aを用いて暗号化し、Aに返送する。

【0126】これを受信したAは、受信データを鍵K_aで復号化する。受信データの復号化方法は、Bの復号化処理と同様であるので、ここでは詳細を省略する。こうして得られたR_b、R_a、K_{ses}の内、R_bおよびR_aが、Aが送信したものと一致するか検証する。この検証に通った場合、AはBを正当なものとして認証する。互いに相手を認証した後には、セッション鍵K_{ses}は、認証後の秘密通信のための共通鍵として利用される。

【0127】なお、受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

【0128】相互認証が成功すれば、上位機器20はサービスセンタ10に対して機器認証開始を制御対象機器（下位機器）30の代理として要求する。サービスセンタ10は要求に応えられる状態であれば、機器認証開始可能であることを上位機器20に通知する。上位機器20はサービスセンタ10に制御対象機器（下位機器）30の機器IDを送信する。ここでサービスセンタ10は下位機器の機器IDの正当性を検証する。正当性の検証は、送付データ中に含まれる機器IDがサービスセンタ10の持つ機器情報データベース106に登録されているか否かをチェックする処理として実行される。機器I

Dの正当性検証が正常に終了すると、上位機器20は制御対象機器（下位機器）30にサービスセンタ10との直接通信の許可を与える。これ以後、上位機器20はサービスセンタ10と制御対象機器（下位機器）30との間の通信内容には関与しない。

【0129】サービスセンタ10との直接通信許可を受けて、制御対象機器（下位機器）30はセンタと直接通信して相互認証を行う。相互認証は、例えば前述の図20、または図22の例のいずれかを用いて実行される。相互認証が完了すると、以後の相互認証時に生成したセッション鍵（共通鍵）を用いてデータが暗号化されて送受信される。セッション鍵の生成はサービスセンタ10、制御対象機器（下位機器）30のどちらが行つてもよい。なお、ここではサービスセンタ10と上位機器20との間および上位機器20と制御対象機器（下位機器）30の間でそれぞれ相互認証が完了しているので、サービスセンタ10と制御対象機器（下位機器）30との直接の相互認証を省略することも可能である。相互認証やセッション鍵の交換が失敗した場合には、センタは下位機器にエラーを返す。すべての処理が完了したならば、サービスセンタ10は制御対象機器（下位機器）30に処理完了を通知する。セッション鍵が制御対象機器（下位機器）30とサービスセンタ10の間で共有できれば、オンライン型下位機器は以降で説明する各手続きにおいて上位機器20と同様に扱うことができる。

【0130】なお、暗号化機能を持たない制御対象機器（下位機器）30の場合には、例えばワントイムパスワードを用いた認証処理により制御対象機器（下位機器）30の認証を実行する。この場合、サービスセンタ10または、上位機器20がセッション鍵を生成して保持し、外部ネットワークを介するサービスセンタ10と上位機器20間のデータ通信をセッション鍵を用いたデータ通信とする。この場合のプロトコルを図23に示す。

【0131】b-2. オフライン型下位機器
次に、オフライン型下位機器の機器認証プロトコルについて説明する。この場合のプロトコルを図24に示す。オフライン型の制御対象機器（下位機器）30は、先に説明したようにメモリーカード等の情報記録媒体を介して制御情報を受け取る構成である。

【0132】オフライン型の制御対象機器（下位機器）30は、最初に情報記録媒体が下位機器に装着されていなければ装着する。その場合には記録媒体の認証を行なう。この認証処理は、制御対象機器（下位機器）30と情報記録媒体の構成（暗号処理機能、鍵格納構成）に応じて、前述の対称鍵、非対称鍵、パスワードを用いた方法等により実行される。記録媒体認証が成功すると、制御対象機器（下位機器）30は機器IDなどの機器認証に必要なデータを情報記録媒体に転送する。転送が終了すると、情報記録媒体を上位機器20に移動する。

【0133】上位機器20は情報記録媒体がセットされ

ると、情報記録媒体の認証を行った後、媒体から機器認証に必要なデータを転送する。情報記録媒体の認証処理は、制御対象機器（下位機器）30と情報記録媒体との認証処理と同様前述の対称鍵、非対称鍵、パスワードを用いた方法等により実行される。転送が終了すると上位機器20と制御対象機器（下位機器）30との相互認証が情報記録媒体の格納データに基づいて実行される。この間、情報記録媒体の上位機器20と制御対象機器（下位機器）30間での移動が必要であれば行う。相互認証が成功すれば、上位機器20はサービスセンタ10に機器認証開始を制御対象機器（下位機器）30に代わって要求する。サービスセンタ10は要求に応えられる状態であれば、機器認証開始可能であることを上位機器20に通知する。

【0134】次に、上位機器20はサービスセンタ10に制御対象機器（下位機器）30の機器IDを送信する。ここでサービスセンタ10は制御対象機器（下位機器）30の機器IDの正当性を検証する。機器IDの正当性検証が正常に終了すれば、制御対象機器（下位機器）30はサービスセンタ20と相互認証処理およびセッション鍵の交換を行う。しかし制御対象機器（下位機器）30とサービスセンタ10とは直接通信できないため、上位機器20、および情報記録媒体が介在して行う。この間、必要に応じて情報記録媒体の上位機器20と制御対象機器（下位機器）30間での移動が行われる。相互認証が完了すると、以後のデータの暗号化に必要なセッション鍵（共通鍵）を生成する。セッション鍵の生成はサービスセンタ10、制御対象機器（下位機器）30のどちらが行つてもよい。なお、暗号化機能を持たない制御対象機器（下位機器）30の場合には、例えばワントイムパスワードを用いた認証処理により制御対象機器（下位機器）30の認証を実行する。この場合、サービスセンタ10または、上位機器20がセッション鍵を生成して保持し、外部ネットワークを介するサービスセンタ10と上位機器20間のデータ通信をセッション鍵を用いたデータ通信とする。相互認証やセッション鍵の交換が失敗した場合には、サービスセンタ10は上位機器20にエラーを返す。すべての処理が完了したならば、サービスセンタ10は上位機器20に処理完了を通知する。上位機器20は情報記録媒体に処理完了通知もしくはエラー通知を転送する。情報記録媒体が制御対象機器（下位機器）30に移動されると、制御対象機器（下位機器）30は情報記録媒体を認証し、記録媒体から処理完了通知もしくはエラー通知を転送（読み出し処理）する。

【0135】[利用者登録、情報変更プロトコル] 次に、利用者名や決済情報などの利用者情報をサービスセンタ10の利用者情報データベース107（図5参照）に登録するための利用者登録、情報変更プロトコルについて説明する。

【0136】a. 上位機器、オンライン型下位機器
まず上位機器 2 0 およびオンライン型の制御対象機器
(下位機器) 3 0 の場合の処理について述べる。この場合のプロトコルを図 2 5 に示す。上位機器 2 0 およびオンライン型の制御対象機器 (下位機器) 3 0 は、「機器」と総称する。機器はサービスセンタ 1 0 に対して利用者登録を行える状態であれば、機器に対して開始確認を通知する。機器は利用者が入力した利用者情報をセッション鍵で暗号化し、機器 I D とともに送信する。利用者情報は、氏名や住所、決済情報などである。決済情報は銀行口座、クレジットカード番号、プリペイドカード番号など、有償サービスの決済に必要な情報である。サービスセンタ 1 0 は暗号化された利用者情報を、機器 I D に対応したセッション鍵で復号する。

【0137】続いてサービスセンタ 1 0 は当該利用者に利用者 I D を発行し、その利用者 I D および利用者情報、機器 I D をサービスセンタ 1 0 は内の利用者情報データベース 1 0 7 に登録する。データベースへの利用者情報の登録後、サービスセンタ 1 0 は利用者 I D をセッション鍵で暗号化し、機器に送信する。機器はこれを受け取ると、暗号化された利用者 I D をセッション鍵で復号する。そして利用者 I D を利用者に通知する。通知は、制御対象機器 (下位機器) 3 0 の例えば表示部 3 0 3 (図 3 参照) において実行される。なお、上位機器において表示することも可能である。ここで利用者が機器を利用するたびに利用者 I D を入力する手間を省くために、利用者 I D を機器に保存しておき、利用者が自分の I D を選択するという方法をとつてもよい。最後にサービスセンタ 1 0 は機器に対して、処理完了通知もしくはエラー通知を行う。

【0138】なお、制御対象機器 (下位機器) 3 0 が暗号化機能を備えない場合は、下位機器と上位機器の間はデータを暗号化せず送信し、上位機器 2 0 がデータをセッション鍵で暗号化した後、サービスセンタ 1 0 に送信する。サービスセンタ 1 0 からのデータは上位機器 2 0 がセッション鍵で復号した後、下位機器に送信する。この場合のプロトコルを図 2 6 に示す。

【0139】なお、すでにサービスセンタ 1 0 内の利用者情報データベース 1 0 7 に利用者情報が登録されており、その情報を変更する場合には、登録手続きの中で利用者 I D を発行すること、および利用者 I D を上位機器に通知する処理が不要となる。また利用者を特定するための氏名等を入力する代わりに、発行された利用者 I D を入力してもよい。この時、サービスセンタ 1 0 は、利用者が利用している機器の機器 I D が当該の利用者 I D と関連づけられていないければ、利用者情報データベース 1 0 7 に機器 I D を追加する処理を実行する。その他の部分は利用者情報登録の場合と同一である。この場合のプロトコルを図 2 7 に示す。

【0140】なお、制御対象機器 (下位機器) 3 0 が暗号化機能を備えない場合は、下位機器と上位機器の間はデータを暗号化せず、上位機器 2 0 がセッション鍵で暗号化した後、サービスセンタ 1 0 にデータ送信を実行する。サービスセンタ 1 0 からのデータは上位機器 2 0 がセッション鍵で復号した後、制御対象機器 (下位機器) 3 0 に送信する。この場合のプロトコルを図 2 8 に示す。

【0141】b. オフライン型下位機器

続いてオフライン型下位機器の場合について述べる。この場合のプロトコルを図 2 9 に示す。記録媒体がオフライン型の制御対象機器 (下位機器) 3 0 に装着されていなければ装着する。その場合には記録媒体の認証が必要となる。制御対象機器 (下位機器) 3 0 は利用者が入力した利用者情報をセッション鍵で暗号化した後、機器 I D とともに記録媒体に転送する。転送が完了した後、情報記録媒体を制御対象機器 (下位機器) 3 0 から取り外し、上位機器 2 0 に装着する。

【0142】上位機器 2 0 は情報記録媒体が装着されると、情報記録媒体の認証を開始する。情報記録媒体の認証が終了した後、上位機器 2 0 は情報記録媒体からデータを転送 (読み取り) する。転送終了後、上位機器 2 0 はサービスセンタ 1 0 に利用者登録開始要求を下位機器の代理として行う。サービスセンタ 1 0 は利用者情報登録を行える状態であれば、上位機器 2 0 に対して開始確認を通知する。

【0143】上位機器 2 0 は制御対象機器 (下位機器) 3 0 からのデータをそのままサービスセンタ 1 0 に送信する。サービスセンタ 1 0 は暗号化された利用者情報を機器 I D に対応したセッション鍵で復号する。続いて当該利用者に利用者 I D を発行し、その利用者 I D および利用者情報、機器 I D を利用者情報データベース 1 0 7 に登録する。

【0144】サービスセンタ 1 0 はデータベースへの利用者情報の登録後、利用者 I D を制御対象機器 (下位機器) 3 0 とのセッション鍵で暗号化し、上位機器 2 0 に送信する。そしてサービスセンタ 1 0 は上位機器 2 0 に対して、処理完了通知もしくはエラー通知を行う。上位機器 2 0 は、サービスセンタ 1 0 から処理完了通知を受け取ると暗号化された利用者 I D を情報記録媒体に転送する。その後、情報記録媒体を上位機器 2 0 から制御対象機器 (下位機器) 3 0 に移動する。情報記録媒体が制御対象機器 (下位機器) 3 0 に装着されると、制御対象機器 (下位機器) 3 0 は情報記録媒体の認証を行う。認証が成功すれば、制御対象機器 (下位機器) 3 0 は情報記録媒体内のデータを転送 (データ読み取り) する。

【0145】次に、制御対象機器 (下位機器) 3 0 は情報記録媒体から読み取った暗号化された利用者 I D をセッション鍵で復号する。そして利用者 I D を利用者に通知する。通知は、制御対象機器 (下位機器) 3 0 の例え

は表示部 3 0 3 (図 4 参照)において実行される。ここで利用者が機器を利用するたびに利用者 ID を入力する手間を省くために、利用者 ID を機器に保存しておき、それを利用者が自分の ID を選択するという方法をとつてもよい。

【0 1 4 6】なお、制御対象機器(下位機器) 3 0 が暗号化機能を備えない場合は、下位機器と上位機器の間はデータを暗号化せず、上位機器 2 0 がセッション鍵で暗号化した後、サービスセンタ 1 0 にデータ送信を実行する。サービスセンタ 1 0 からのデータは上位機器 2 0 がセッション鍵で復号した後、制御対象機器(下位機器) 3 0 に送信する。この場合のプロトコルを図 3 0 に示す。

【0 1 4 7】なお、すでにサービスセンタ 1 0 内の利用者情報データベース 1 0 7 に利用者情報が登録されており、その情報を変更する場合には、登録手続きの中で利用者 ID を発行すること、および利用者 ID を上位機器に通知する処理が不要となる。また利用者を特定するための氏名等を入力する代わりに、発行された利用者 ID を入力してもよい。この時、サービスセンタ 1 0 は、利用者が利用している機器の機器 ID が当該の利用者 ID と関連づけられていなければ、利用者情報データベース 1 0 7 に機器 ID を追加する処理を実行する。その他の部分は利用者情報登録の場合と同一である。この場合のプロトコルを図 3 1 に示す。

【0 1 4 8】なお、制御対象機器(下位機器) 3 0 が暗号化機能を備えない場合は、下位機器と上位機器の間はデータを暗号化せず、上位機器 2 0 がセッション鍵で暗号化した後、サービスセンタ 1 0 にデータ送信を実行する。サービスセンタ 1 0 からのデータは上位機器 2 0 がセッション鍵で復号した後、制御対象機器(下位機器) 3 0 に送信する。この場合のプロトコルを図 3 2 に示す。

【0 1 4 9】【利用者認証情報登録プロトコル】利用者を識別するためにはいくつかの方法が考えられるが、ここではパスワードを用いた方法と ID カードを用いた場合について説明する。ID カードを用いる場合には、個人別の ID を埋め込んだカード、指紋などの生体情報を認識できる機構を備えたカード、あるいは利用者個人の公開鍵・秘密鍵の組を保存しているカードなどを用いることが可能である。ID カードとしては磁気テープを有する接触型カードや、無線通信を行う非接触型カードのどちらを用いててもよい。また、利用者を識別するための利用者認証情報を保存し照合を行う場所としては、機器(上位機器・制御対象機器(下位機器))あるいはサービスセンタが考えられる。機器に保存する場合は機器における利用者の制限などの管理を個別に行なうことが容易である。サービスセンタに登録する場合には複数の機器を利用する場合においても、機器ごとに登録作業を行う必要がない。まずはパスワード等、認証のための情報を機

器もしくはセンタに登録する手続きについて述べる。

【0 1 5 0】a. 機器に保存

利用者のパスワード等の利用者認証情報を機器内部に保存して、サービスの提供等の際に利用者の入力した利用者認証情報と照合する方法である。この場合におけるパスワードの登録について説明する。この場合のプロトコルを図 3 3 に示す。機器は利用者が入力した利用者 ID を受け取ると、利用者に対してパスワードの入力を促す。

【0 1 5 1】利用者がパスワードを操作部(上位機器の場合、操作部 2 0 9、下位機器の場合操作部 3 0 8)から入力すると、機器は利用者 ID と対応するパスワードの組を機器内部のメモリに保存する。この時、パスワードを平文のまま保存するのではなく暗号化を施してもよい。次に、サービスセンタ 1 0 は機器に対して、処理完了もしくはエラーを通知する。

【0 1 5 2】次に ID カードを用いる利用者認証情報登録処理について説明する。この場合のプロトコルを図 3 4 に示す。機器は利用者が ID カードをセットすると、ID カードから利用者 ID および利用者認証情報を転送する。機器は利用者 ID と対応する利用者認証情報を機器内部のメモリに保存する。次にサービスセンタ 1 0 は機器に対して、処理完了もしくはエラーを通知する。

【0 1 5 3】b. センタに保存(上位機器・オンライン型下位機器)

利用者認証情報をサービスセンタ 1 0 に保存して、サービスの提供等の際に利用者の入力した利用者認証情報と照合する方法である。この場合におけるパスワードの登録について説明する。この場合のプロトコルを図 3 5 に示す。

【0 1 5 4】まず上位機器およびオンライン型の制御対象機器(下位機器)を利用する場合は以下の通りである。機器はサービスセンタ 1 0 に利用者認証情報の登録開始を要求する。サービスセンタ 1 0 は要求に応えられる状態であれば、登録開始可能であることを機器に通知する。機器は利用者が入力した利用者 ID を受け取ると、利用者に対してパスワードの入力を促す。利用者がパスワードを入力すると、機器は利用者 ID と対応するパスワードの組をセッション鍵で暗号化し、機器 ID とともにサービスセンタ 1 0 に送信する。サービスセンタ 1 0 は暗号化された利用者 ID とパスワードを機器 ID に対応したセッション鍵で復号する。統いて、パスワードを利用者情報データベース 1 0 7 に登録する。セッション鍵での復号やデータベースへの登録が失敗した場合には、サービスセンタ 1 0 は機器にエラーを返す。すべての処理が完了したならば、サービスセンタ 1 0 は機器に処理完了を通知する。

【0 1 5 5】なお、制御対象機器(下位機器) 3 0 が暗号化機能を備えない場合は、下位機器と上位機器の間はデータを暗号化せず、上位機器 2 0 がセッション鍵で暗

号化した後、サービスセンタ10にデータ送信を実行する。サービスセンタ10からのデータは上位機器20がセッション鍵で復号した後、制御対象機器（下位機器）30に送信する。この場合のプロトコルを図36に示す。

【0156】次に、IDカードを用いる方法について説明する。この場合のプロトコルを図37に示す。機器は利用者がIDカードをセットすると、IDカードから利用者IDおよび利用者認証情報を転送する。機器はサービスセンタ10に利用者認証情報の登録開始を要求する。サービスセンタ10は要求に応えられる状態であれば、登録開始可能であることを機器に通知する。その後、機器は利用者IDと対応する利用者認証情報の組をセッション鍵で暗号化し、機器IDとともにサービスセンタ10に送信する。以下の処理はパスワードを用いる場合と同様である。

【0157】なお、制御対象機器（下位機器）30が暗号化機能を備えない場合は、下位機器と上位機器の間はデータを暗号化せず、上位機器20がセッション鍵で暗号化した後、サービスセンタ10にデータ送信を実行する。サービスセンタ10からのデータは上位機器20がセッション鍵で復号した後、制御対象機器（下位機器）30に送信する。この場合のプロトコルを図38に示す。

【0158】c. オフライン型下位機器
次にオフライン型の制御対象機器（下位機器）の場合の利用者認証情報登録プロトコルについて述べる。まず、この場合におけるパスワードの登録について説明する。この場合のプロトコルを図39に示す。

【0159】オフライン型の制御対象機器（下位機器）30は利用者に利用者IDおよびパスワードの入力を促す。利用者IDおよびパスワードが入力されると、制御対象機器（下位機器）30はこれをセッション鍵で暗号化して機器IDとともに情報記録媒体に転送する。情報記録媒体が下位機器から上位機器に移されるとき、上位機器20は情報記録媒体の認証を行う。情報記録媒体の認証が成功すれば、上位機器20は情報記録媒体からデータを転送する。その後、上位機器20はサービスセンタ10に利用者認証情報の登録開始を要求する。サービスセンタ10は要求に応えられる状態であれば、登録開始可能であることを上位機器20に通知する。上位機器20は情報記録媒体から転送（読み出し）したデータをそのままセンタに送信する。サービスセンタ10は暗号化された利用者IDとパスワードを機器IDに対応したセッション鍵で復号する。統いて、パスワードを利用者情報データベース107に登録する。セッション鍵での復号やデータベースへの登録が失敗した場合には、サービスセンタ10は上位機器20にエラーを返す。すべての処理が完了したならば、サービスセンタ10は上位機器20に処理完了を通知する。サービスセンタ10から上

位機器20に対するエラー通知、処理完了通知は情報記録媒体を介してオフライン型の制御対象機器（下位機器）30に転送される。

【0160】なお、制御対象機器（下位機器）30が暗号化機能を備えない場合は、下位機器と上位機器の間はデータを暗号化せず、上位機器20がセッション鍵で暗号化した後、サービスセンタ10にデータ送信を実行する。サービスセンタ10からのデータは上位機器20がセッション鍵で復号した後、制御対象機器（下位機器）30に送信する。この場合のプロトコルを図40に示す。

【0161】次に、IDカードを用いる利用者認証情報登録プロトコルについて説明する。この場合のプロトコルを図41に示す。制御対象機器（下位機器）30は利用者がIDカードをセットすると、IDカードから利用者IDおよび利用者認証情報を転送する。以下の処理はパスワードを用いる場合と同様である。

【0162】なお、制御対象機器（下位機器）30が暗号化機能を備えない場合は、下位機器と上位機器の間はデータを暗号化せず、上位機器20がセッション鍵で暗号化した後、サービスセンタ10にデータ送信を実行する。サービスセンタ10からのデータは上位機器20がセッション鍵で復号した後、制御対象機器（下位機器）30に送信する。この場合のプロトコルを図42に示す。

【0163】【利用者認証プロトコル】次に、利用者認証情報登録プロトコルで登録した利用者認証情報を用いて、利用者を認証する手続きについて述べる。

【0164】a. 機器に利用者認証情報を保存
利用者の利用者認証情報を機器に保存して、サービスの提供等の際に利用者の入力した利用者認証情報を照合する場合の利用者認証の方法について説明する。

【0165】利用者認証情報としてパスワードを利用する場合のプロトコルを図43に示す。機器は利用者が入力した利用者IDを受け取ると、利用者に対してパスワードの入力を促す。利用者がパスワードを入力すると、機器はメモリに保存されている利用者IDとパスワードの組の中から、利用者IDに対応したパスワードを選び出し、これと入力されたパスワードを照合する。照合に成功すれば利用者は正当な権限を有すると見え、サービス等を受けることが可能となる。照合に失敗した場合はエラー処理を行う。

【0166】次にIDカードを用いる方法について説明する。この場合のプロトコルを図44に示す。機器は利用者がIDカードをセットすると、IDカードから利用者IDおよび利用者認証情報を転送する。この後、機器は内部のメモリに保存されている利用者IDと利用者認証情報の組の中から、利用者IDに対応した利用者認証情報を選び出し、IDカードから転送した利用者認証情報を照合する。照合に成功すれば利用者は正当な権限を

有すると言え、サービス等を受けることが可能となる。照合に失敗した場合はエラー処理を行う。

【0167】b. センタに利用者認証情報を保存

利用者のパスワードをサービスセンタ10に保存して、サービスの提供等の際に利用者の入力したパスワードと照合する場合の利用者認証の方法について説明する。パスワードを利用する場合のプロトコルを図45に示す。機器はサービスセンタ10に利用者認証開始を要求する。サービスセンタ10は要求に応えられる状態であれば、認証開始可能であることを機器に通知する。機器は利用者が入力した利用者IDを受け取ると、利用者に対してパスワードの入力を促す。利用者がパスワードを入力すると、機器は利用者IDと対応するパスワードの組をセッション鍵で暗号化した上で機器IDと共にセンタに送信する。センタは暗号化された利用者IDとパスワードを機器IDに対応したセッション鍵で復号する。サービスセンタ10は機器、利用者情報データベース10に登録されたパスワードと、機器から送信されたパスワードとを照合する。サービスセンタ10は照合結果を機器に送信する。照合に成功すれば利用者は正当な権限を有すると言え、サービス等を受けることが可能となる。利用者情報データベース10の当該利用者IDのエントリに送信された機器IDが含まれていない場合には追加する。このことにより利用者が複数の機器を利用する場合にも、利用者IDと機器IDとを関連づけることが可能である。照合に失敗した場合はエラー処理を行う。

【0168】なお、制御対象機器（下位機器）30が暗号化機能を備えない場合は、下位機器と上位機器の間はデータを暗号化せず、上位機器20がセッション鍵で暗号化した後、サービスセンタ10にデータ送信を実行する。サービスセンタ10からのデータは上位機器20がセッション鍵で復号した後、制御対象機器（下位機器）30に送信する。この場合のプロトコルを図46に示す。

【0169】次に、IDカードを用いた利用者認証の方法について説明する。この場合のプロトコルを図47に示す。機器は利用者がIDカードをセットすると、IDカードから利用者IDおよび利用者認証情報を転送する。機器はサービスセンタ10に利用者認証開始を要求する。サービスセンタ10は要求に応えられる状態であれば、認証開始可能であることを機器に通知する。機器は利用者IDと対応する利用者認証情報の組をセッション鍵で暗号化した上で機器IDと共にサービスセンタ10に送信する。サービスセンタ10は暗号化された利用者IDと利用者認証情報を機器IDに対応したセッション鍵で復号する。サービスセンタ10は利用者情報データベース10に登録された利用者認証情報と、機器から送信された利用者認証情報を照合する。さらに、サービスセンタ10は照合結果を機器に送信する。照合に

成功すれば利用者は正当な権限を有すると言え、サービス等を受けることが可能となる。利用者情報データベース10の当該利用者IDのエントリに送信された機器IDが含まれていない場合には追加する。照合に失敗した場合はエラー処理を行う。

【0170】なお、制御対象機器（下位機器）30が暗号化機能を備えない場合は、下位機器と上位機器の間はデータを暗号化せず、上位機器20がセッション鍵で暗号化した後、サービスセンタ10にデータ送信を実行する。サービスセンタ10からのデータは上位機器20がセッション鍵で復号した後、制御対象機器（下位機器）30に送信する。この場合のプロトコルを図48に示す。

【0171】c. オフライン型の下位機器の場合

次にオフライン型の制御対象機器（下位機器）30の場合の利用者認証の方法について説明する。パスワードを利用する場合のプロトコルを図49に示す。オフライン型の制御対象機器（下位機器）30は利用者IDとパスワードを入力を促す。利用者IDおよびパスワードが入力されれば、制御対象機器（下位機器）30はこれをセッション鍵で暗号化して機器IDとともに情報記録媒体に転送する。

【0172】情報記録媒体が制御対象機器（下位機器）30から上位機器20に移されると、上位機器20は情報記録媒体の認証を行う。情報記録媒体の認証が成功すれば、上位機器20は情報記録媒体からデータを転送（読み取り）する。そして、上位機器20はサービスセンタ10に利用者認証開始を要求する。サービスセンタ10は要求に応えられる状態であれば、認証開始可能であることを上位機器20に通知する。通知を受領すると上位機器20は情報記録媒体から転送したデータをそのままサービスセンタ10に送信する。サービスセンタ10は暗号化された利用者IDとパスワードを機器IDに対応したセッション鍵で復号する。サービスセンタ10は利用者情報データベース10に登録された利用者認証情報と、機器から送信された利用者認証情報を照合する。サービスセンタ10は照合結果を上位機器20に送信する。照合に成功すれば利用者は正当な権限を有すると言え、サービス等を受けることが可能となる。利用者情報データベースの当該利用者IDのエントリに送信された機器IDが含まれていない場合には追加する。照合に失敗した場合はエラー処理を行う。認証結果を受け取った上位機器20は、情報記録媒体にその結果を転送する。情報記録媒体が上位機器20から制御対象機器（下位機器）30に移されると、制御対象機器（下位機器）30は情報記録媒体の認証を行う。認証結果が成功すれば、下位機器は情報記録媒体からデータを転送（読み取り）する。制御対象機器（下位機器）30は認証結果を利用者に、例えば表示部303を介して通知する。

【0173】なお、制御対象機器（下位機器）30が暗号化機能を備えない場合は、下位機器と上位機器の間はデータを暗号化せず、上位機器20がセッション鍵で暗号化した後、サービスセンタ10にデータ送信を実行する。サービスセンタ10からのデータは上位機器20がセッション鍵で復号した後、制御対象機器（下位機器）30に情報記録媒体を介して送信する。この場合のプロトコルを図50に示す。

【0174】次にオフライン型の制御対象機器（下位機器）30の場合におけるIDカードを用いた利用者認証の方法について説明する。この場合のプロトコルを図51に示す。オフライン型の制御対象機器（下位機器）30は利用者がIDカードをセッピトすると、IDカードから利用者IDおよび利用者認証情報を転送する。以下の処理はパスワードを用いる場合と同様である。

【0175】なお、制御対象機器（下位機器）30が暗号化機能を備えない場合は、下位機器と上位機器の間はデータを暗号化せず、上位機器20がセッション鍵で暗号化した後、サービスセンタ10にデータ送信を実行する。サービスセンタ10からのデータは上位機器20がセッション鍵で復号した後、制御対象機器（下位機器）30に情報記録媒体を介して送信する。この場合のプロトコルを図52に示す。

【0176】【サービスプロトコル】次に、サービスセンタ10から上位機器20を利用した遠隔サービスの提供処理について説明する。

【0177】a. センター上位機器、センター上位機器一下位機器（オンライン）

まず、サービスセンタ10と上位機器20、オンライン型の制御対象機器（下位機器）30を利用する場合のプロトコルを図53に示す。ここでは、機器といった場合、上位機器20と、オンライン型の制御対象機器（下位機器）30とを含む総称である。

【0178】最初に機器はサービスセンタ10にサービス開始を要求する。サービスセンタ10は要求に応えられる状態であれば、サービス開始可能であることを機器に通知する。サービスはサービスセンタ10と機器との間でデータを通信することにより実施される。サービスセンタ10からサービス提供のためのデータが送信される場合について述べる。

【0179】まずサービスセンタのCPU101の制御によりサービス提供用データベース103から、例えばメンテナンス情報のようなサービス用データが暗号化通信IC104に送られる。暗号化通信IC104は、そのデータを機器認証の際にサービスセンタと機器との間で交換したセッション鍵により暗号化を施した後、外部ネットワークに送信する。

【0180】上位機器20側では、暗号化通信IC205が外部ネットワークインターフェース208経由で受信

したデータをセッション鍵を用いて復号する。復号されたデータはデータバスを通じてメモリ202やディスク等の記録装置210に転送される。CPU201はメモリ202やディスク等の記録装置210からデータを読み出して、機器固有部204の制御を行う。なお、オンライン型の制御対象機器（下位機器）30の制御を行なう場合は、上位機器20と制御対象機器（下位機器）30間でデータが転送される。

【0181】続いてオンライン型の制御対象機器（下位機器）30からサービスセンタ10にデータを送信する場合について述べる。まず、オンライン型の制御対象機器（下位機器）30のCPU3001の制御によりデータが暗号化通信IC305に送られる。暗号化通信IC305はデータのセッション鍵による暗号化を施した後、ローカルインターフェース307を介して上位機器20に送信する。上位機器20は制御対象機器（下位機器）30からローカルインターフェース208を介して受信したデータを外部ネットワークインターフェース208を経由して外部ネットワークに送信する。

【0182】サービスセンタ10側では、暗号化通信IC104が外部ネットワークインターフェース105経由で受信したデータをセッション鍵を用いて復号する。復号されたデータはデータバスを通じて、メモリ102やサービス提供用データベース103、機器情報データベース106、利用者情報データベース107に転送される。サービスを提供している間、必要であればサービスセンタ10のCPU101は課金情報をメモリ102もしくは利用者情報データベース107に記録する。課金情報とは有償サービスの利用回数や時間、送受信データ量などである。

【0183】以上、説明したように、サービスの提供中にサービスセンタ10と機器との間で行われるデータの通信は、セッション鍵を用いて暗号化されているので通信内容の保護が可能となる。サービスの提供が終了すれば、サービスセンタ10のCPU101は利用者IDを検索キーとして利用者データベースから利用者の決済情報を取得し、決済処理を行う。サービスの提供を終了する際には、終了処理を行う。

【0184】なお、制御対象機器（下位機器）30が暗号化機能を備えない場合は、下位機器と上位機器の間はデータを暗号化せず、上位機器20がセッション鍵で暗号化した後、サービスセンタ10にデータ送信を実行する。サービスセンタ10からのデータは上位機器20がセッション鍵で復号した後、制御対象機器（下位機器）30に送信する。この場合のプロトコルを図54に示す。

【0185】2. センター上位機器一下位機器（オフライン）

次に、オフライン型下位機器に対する遠隔サービスの提供処理について説明する。この場合、サービスはサービ

センタ 1 0 と上位機器 2 0 の間で通信を行い、上位機器 2 0 がオフライン型の制御対象機器（下位機器）3 0 の代わりにデータを受信して一度保存し、そのデータを情報記録媒体を用いてまとめて下位機器に転送することにより実施される。この場合のプロトコルを図 5 5 に示す。

【0186】最初に情報記録媒体が制御対象機器（下位機器）3 0 に装着されなければ装着する。その場合には情報記録媒体の認証が必要となる。情報記録媒体の認証が成功すると、制御対象機器（下位機器）3 0 はサービス名やパラメータなど、サービス開始に必要なデータを媒体に転送する。転送が終了してから、情報記録媒体を上位機器 2 0 に移動する。

【0187】上位機器 2 0 は情報記録媒体がセットされると、情報記録媒体認証を行った後、情報記録媒体からサービス開始に必要なデータを転送する。転送が終了すると上位機器 2 0 はサービスセンタ 1 0 にサービス開始を要求する。サービスセンタ 1 0 は要求に応えられる状態であれば、サービス開始可能であることを上位機器 2 0 に通知する。

【0188】サービス提供中にデータを上位機器 2 0 と制御対象機器（下位機器）3 0 の間でやりとりする場合について述べる。上位機器 2 0 が情報記録媒体にデータを転送する場合、記録媒体認証が済んでいなければ、上位機器 2 0 の暗号化通信 I C 2 0 5 は情報記録媒体の認証を開始する。情報記録媒体が認証できれば、上位機器 2 0 の C P U 2 0 1 はサービスセンタ 1 0 から制御対象機器（下位機器）3 0 のために受信したデータを上位機器 2 0 内部の記録装置 2 1 0 から読み出し、暗号化通信 I C 2 0 5 に転送する。暗号化通信 I C 2 0 5 に転送されたデータはそのまま記録媒体インターフェース 2 0 7 を経由して情報記録媒体 2 1 1 に転送（書き込み）される。

【0189】制御対象機器（下位機器）3 0 が情報記録媒体にデータを転送する場合、記録媒体認証が済んでいなければ、制御対象機器（下位機器）3 0 の暗号化通信 I C 3 0 5 は情報記録媒体の認証を開始する。情報記録媒体が認証できれば、制御対象機器（下位機器）3 0 の C P U 3 0 1 はメモリ 3 0 2 もしくは記録装置 3 0 9 からデータを読み出し、暗号化通信 I C 3 0 5 に転送する。暗号化通信 I C 3 0 5 は転送されたデータをセッション鍵で暗号化し、記録媒体インターフェース 3 0 6 経由で情報記録媒体 3 1 0 に転送する。

【0190】またサービス提供中にデータをサービスセンタ 1 0 と上位機器 2 0 の間でやりとりする場合について述べる。サービスセンタ 1 0 からサービス提供のためのデータが送信される場合について述べる。最初にサービスセンタ 1 0 の C P U 1 0 1 の制御によりサービス提供用データベース 1 0 3 からデータが暗号化通信 I C 1 0 4 に送られる。暗号化通信 I C 1 0 4 は、そのデータ

を機器認証の際にサービスセンタ 1 0 と制御対象機器（下位機器）3 0 との間で交換したセッション鍵により暗号化を施した後、外部ネットワークインターフェース 1 0 5 を経由して外部ネットワークに送信する。

【0191】上位機器 2 0 側では、暗号化通信 I C 2 0 5 が外部ネットワークインターフェース 2 0 8 経由でデータを受信し、データバスを通じてメモリ 2 0 2 やディスク等の記録装置 2 1 0 に転送する。

【0192】続いて上位機器 2 0 からサービスセンタ 1 0 にデータを送信する場合について述べる。まず、上位機器 2 0 の C P U 2 0 1 の制御により制御対象機器（下位機器）3 0 とサービスセンタ 1 0 との間で交換されたセッション鍵で暗号化されたデータは、メモリ 2 0 2 もしくは記録装置 2 1 0 から読み出されて暗号化通信 I C 2 0 5 に送られる。暗号化通信 I C 2 0 5 はそのデータを外部ネットワークインターフェース 2 0 6 を経由して外部ネットワークに送信する。サービスセンタ 1 0 側では、暗号化通信 I C 1 0 4 が外部ネットワークインターフェース 1 0 5 経由で受信したデータをセッション鍵を用いて復号する。復号されたデータはデータバスを通じて、メモリ 1 0 2 やサービス提供用データベース 1 0 3、機器情報データベース 1 0 6、利用者情報データベース 1 0 7 に転送される。サービスを提供している間、必要であればサービスセンタ 1 0 の C P U 1 0 1 は課金情報をメモリ 1 0 2 もしくは利用者情報データベース 1 0 7 に記録する。課金情報とは有償サービスの利用回数や時間、送信データ量などである。

【0193】以上のように、サービスの提供中にサービスセンタと機器との間で行われるデータの通信は、セッション鍵を用いて暗号化され通信内容を保護することができる。サービスの提供が終了すれば、サービスセンタ 1 0 の C P U 1 0 1 は利用者 I D を検索キーとして利用者データベース 1 0 7 から利用者の決済情報を取得し、決済処理を行う。サービスの提供を終了する際には、終了処理を行う。

【0194】なお、制御対象機器（下位機器）3 0 が暗号化機能を備えない場合は、下位機器と上位機器の間はデータを暗号化せず、上位機器 2 0 がセッション鍵で暗号化した後、サービスセンタ 1 0 にデータ送信を実行する。サービスセンタ 1 0 からのデータは上位機器 2 0 がセッション鍵で復号した後、制御対象機器（下位機器）3 0 に情報記録媒体を介して送信する。この場合のプロトコルを図 5 6 に示す。

【0195】【具体的な処理例】以下、本発明の通信手段を介したサービス提供システムおよびサービス提供方法の具体的なサービス提供例について説明する。

【0196】＜リモートメンテナンス＞まず、具体的なサービス提供例として、遠隔診断・修復システムについて述べる。この場合のプロトコルを図 5 7 に示す。このシステムは、機器に障害が発生した場合に、障害個所の

診断及び修復をサービスセンタ10からの操作により行う例である。

【0197】まず機器の状態を調べるために診断を行う。この診断は、機器のCPU（上位機器の場合はCPU201、下位機器の場合はCPU301）が機器内部の様々な部分に対して命令を発行してその応答を分析することによっておこなう。診断のためのプログラムは機器内部のメモリやディスク等に予め記録しておく。診断が終了すれば、その結果をサービスセンタ10に送信する。あるいはセンタの助けを借りて診断を行う構成としてもよい。この場合、機器はサービスセンタ10に対して診断依頼のメッセージを送信する。診断依頼のメッセージを受け取ったサービスセンタ10は、該当機器の診断が可能であれば診断命令を発行し、機器に対して送信する。機器はサービスセンタ10から診断命令を受け取るとその命令を実行し、結果をサービスセンタ10に送信する。

【0198】サービスセンタ10は機器から送信された結果を分析し、それによって必要ならば再度診断命令を発行し、機器に送信する。サービスセンタ10が診断が終了したと判断するまで、上記診断命令の発行から分析の手順を繰り返す。以上のように遠隔診断を行って障害箇所および状態を特定でき、かつ遠隔修復が可能であれば修復の手続きに入る。遠隔修復は診断結果に基づき、サービスセンタ10が機器の障害を復旧するために必要な修復命令を機器に送信することにより行われる。

【0199】サービスセンタ10のCPU1001は診断結果を分析して、修復命令を発行する。この際サービス提供用データベース103に蓄積された該当機器あるいは同機種の過去の障害履歴を参照して、最適な命令を選択する。サービスセンタ10はこの修復命令を機器に送信する。機器は受信した修復命令を機器内のCPUの制御により実行してその結果をセンタに送信する。結果を受信したサービスセンタは、その結果や過去の履歴に基づいて分析を行い、必要ならば再度修復命令を発行し、機器に送信する。必要に応じて利用者へのメッセージを機器の表示部に表示する。そして修復の実行を続けるなどの入力を求める。センタが修復が完了したと判断する、あるいは利用者が修復を終了するまで、上記修復命令の発行から分析の手順を繰り返す。修復を終了する際には、それまでの診断結果および修復内容を機器情報データベース106に登録する。データベースに登録された診断結果および修復内容は課金に利用したり、複数の機器のデータをまとめて機器メーカーへフィードバックして機器の改善に役立てたりすることができる。そしてセンタは機器に対して遠隔修復の終了を通知する。

【0200】<バックアップ・リストア>本発明の別のサービス提供例として、機器に保存されているデータのバックアップおよびリストア処理をサービスセンタ10が実行する処理構成について説明する。

【0201】これは、機器に保存されている設定情報等のデータをあらかじめサービスセンタ10の記憶手段にバックアップしておき、データが万一消してもリストアすることで、その機器を以前の状態のまま利用できるようにするためのものである。最初にバックアップについて説明する。この場合のプロトコルを図58に示す。

【0202】機器はサービスセンタ10に対してバックアップ開始要求を行う。この要求を受信したサービスセンタ10は、サービス提供用データベース103上にバックアップのための領域の確保を行う。領域確保が成功し、かつバックアップを行える状態にあれば、サービスセンタ10は機器に対してバックアップ開始確認通知を送信する。開始確認通知を受信した機器は、バックアップ対象のデータをサービスセンタ10に送信する。サービスセンタ10は受信したバックアップデータを確保した領域に保存する。保存が終了すると、機器情報データベース106にバックアップ日時や保存領域などのバックアップ情報を登録する。そしてサービスセンタ10は機器に対してバックアップの終了を通知する。

【0203】統一リストアの手順について説明する。この場合のプロトコルを図59に示す。機器はサービスセンタ10に対してリストア開始要求を行う。この要求を受信したサービスセンタ10は、機器IDを検索キーとして機器情報データベース106からバックアップ情報を取得する。バックアップ情報の取得に成功し、かつリストアを行える状態にあれば、サービスセンタ10は機器に対してリストア開始確認通知を送信する。そしてサービスセンタ10は、バックアップ情報からバックアップデータが保存されているサービス提供用データベース103上の領域情報を取り出す。この情報に基づきサービス提供用データベース103上の領域からバックアップデータを読み出し、機器に送信する。

【0204】機器は受信したバックアップデータをチェックした後、リストアを実行する。リストアが終了すると、機器はサービスセンタ10に対してリストアの終了を通知する。リストア終了通知を受信したサービスセンタ10は、機器情報データベース106にリストア履歴を登録する。そしてサービスセンタ10は機器に対してリストアに関する処理の終了を通知する。

【0205】<データ配信（音楽、映像、文字情報など）>本発明のさらに別のサービス提供例として、データ配信について述べる。

【0206】これは、音楽や映像、文字情報などのデータをサービスセンタ10に蓄積し、利用者の要求に応じてサービスセンタ10から機器に取り込んで利用できるものである。この場合のプロトコルを図60に示す。データ配信機能を利用する場合には、まず利用者は機器に設けられた操作部（上位機器の場合は操作部209、下位機器の場合は操作部308）でデータ配信を開始する操作を行う。利用者からの入力を受け付けた機器はサー

サービスセンタ10に対してデータ配信開始要求を行う。サービスセンタ10は、データ配信を行える状態にあれば、機器に対してデータ配信開始確認通知を送信する。開始確認通知を受信した機器は、表示部（上位機器の場合は表示部203、下位機器の場合は表示部303）にデータ配信開始のメッセージを表示する。さらにサービスセンタ10は利用可能なデータに関する選択肢を含んだメニューを機器に送信する。機器はこのメニューを受信すると、表示部に表示する。

【0207】利用者がメニューの中から必要なデータを選択して操作部に入力すると、機器は選択されたデータが何であるかという情報、たとえばデータ番号をサービスセンタ10に送信する。サービスセンタ10は、サービス提供用データベースから必要なデータを取得し、機器に送信する。機器はデータを受信したことを表示部に表示する。そして利用者はデータを再生するなどの操作を行う。利用者が引き続きデータ配信機能を利用する場合には、操作部から必要な入力を行えばよい。データ配信が終了すると、サービスセンタ10は、必要であれば機器情報データベース106にデータ配信履歴を登録する。データベースに登録されたデータ配信履歴は課金に利用したり、複数の機器のデータをまとめて以後提供するデータの検討などのマーケティングに役立てたりすることが可能である。そしてサービスセンタ10は機器に対してデータ配信の終了を通知する。

【0208】<ヘルプ・チュートリアル>さらに、本発明の別のサービス提供例として、機器の操作方法を解説するヘルプ機能を提供する例について述べる。これは、機器の操作方法を解説するヘルプデータをサービスセンタ10に蓄積し、利用者の要求に応じて必要な部分を機器に取り込んで、利用者に提示するものである。この場合のプロトコルを図61に示す。

【0209】このヘルプ機能に関しては、機器にすべてのヘルプデータを保存しておくことも可能であるが、機器には保存のための領域が少ない場合があることや、常に新しいヘルプデータを保持することが困難なことから、全部あるいは一部のヘルプデータをサービスセンタ10に置く形態とする例である。ヘルプ機能を利用する場合には、まず利用者は操作部（上位機器の場合は操作部209、下位機器の場合は操作部308）でヘルプを開始する操作を行う。利用者からの入力を受け付けた機器はサービスセンタ10に対してヘルプ開始要求を行う。ヘルプデータの提供を行える状態にあれば、サービスセンタ10は機器に対してヘルプ開始確認通知を送信する。

【0210】開始確認通知を受信した機器は、ヘルプの必要な部分を指定するデータをサービスセンタ10に送信する。これを受信したサービスセンタ10は、サービス提供用データベース103から必要なヘルプデータを取得し、機器に送信する。機器は受信したヘルプデータ

を表示部（上位機器の場合は表示部203、下位機器の場合は表示部303）に表示する。利用者が引き続きヘルプ機能を利用する場合に、操作部から必要な入力を行えればよい。ヘルプデータの提供が終了すると、機器情報データベースにヘルプ提供履歴を登録する。そしてセンタは機器に対してヘルプの終了を通知する。

【0211】また単純なヘルプだけではなく、チュートリアルを提供する、すなわち操作情報を提供する構成とすることも可能である。これは利用者が機器の利用方法を習得するための機能であり、機器の各部分を操作するとその状況に応じて、表示や操作形態が変化する。この場合のプロトコルを図62に示す。チュートリアル機能を利用する場合には、まず利用者は操作部でチュートリアルを開始する操作を行う。利用者からの入力を受け付けた機器はセンタに対してチュートリアル開始要求を行う。チュートリアルを行える状態にあれば、センタは機器に対してチュートリアル開始確認通知を送信する。開始確認通知を受信した機器は、表示部にチュートリアル開始のメッセージを表示する。利用者が機器の操作を行うと、機器は操作内容と機器の内部状態をサービスセンタ10に送信する。サービスセンタ10はこれらの情報に基づいて、次に提供すべきデータを決定する。そして、サービス提供用データベースから必要なチュートリアルデータを取得し、機器に送信する。

【0212】機器は受信したチュートリアルデータを表示部に表示する。利用者が引き続きチュートリアル機能を利用する場合には、操作部から必要な入力を行えよ。チュートリアルデータの提供が終了すると、機器情報データベースにチュートリアル提供履歴を登録する。そしてセンタは機器に対してチュートリアルの終了を通知する。

【0213】以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参考すべきである。

【0214】

【発明の効果】以上説明してきたように、本発明の通信手段を介したサービス提供システム、サービス提供方法、およびサービス仲介装置、並びにプログラム提供媒体によれば、機器がサービスセンタと直接接続できない構成であった場合でも、通信手段を有する上位機器からローカルネットワークまたは情報記録媒体を介してサービスセンタからの情報を受け取ることが可能となり、制御、メンテナンス等の必要な制御対象機器（下位機器）のすべてに外部ネットワークに接続するための通信インターフェース等の通信手段を構成することが必要とならない。

【0 2 1 5】さらに、本発明の通信手段を介したサービス提供システム、サービス提供方法、およびサービス仲介装置、並びにプログラム提供媒体によれば、制御、メントナンス等の必要な制御対象機器（下位機器）が暗号化機能を備えない構成であっても、制御対象機器（下位機器）とローカルネットワークまたは情報記録媒体を介して通信可能な上位機器がデータを暗号化した上でサービスセンタとの通信処理を実行するため、通信データの安全性が保証されていない公衆ネットワークを経由しても、制御情報、あるいは制御情報を提供するために必要な個人情報などの重要な情報の漏洩が防止可能となる。

【図面の簡単な説明】

【図 1】本発明の通信手段を介したサービス提供システムのシステム概要を示す図である。

【図 2】本発明の通信手段を介したサービス提供システムを構成する上位機器の構成を示す図である。

【図 3】本発明の通信手段を介したサービス提供システムを構成する下位機器（オンライン型）の構成を示す図である。

【図 4】本発明の通信手段を介したサービス提供システムを構成する下位機器（オフライン型）の構成を示す図である。

【図 5】本発明の通信手段を介したサービス提供システムを構成するサービスセンタの構成を示す図である。

【図 6】本発明の通信手段を介したサービス提供システムにおけるデータ通信の暗号化・認証レベルを示す図である。

【図 7】本発明の通信手段を介したサービス提供システムにおける処理全体を説明するフローチャート（その1）である。

【図 8】本発明の通信手段を介したサービス提供システムにおける処理全体を説明するフローチャート（その2）である。

【図 9】本発明の通信手段を介したサービス提供システムにおける処理全体を説明するフローチャート（その3）である。

【図 10】本発明の通信手段を介したサービス提供システムにおける処理全体を説明するフローチャート（その4）である。

【図 11】本発明の通信手段を介したサービス提供システムにおける機器登録プロトコルを説明する図（その1）である。

【図 12】本発明の通信手段を介したサービス提供システムにおける機器登録プロトコルを説明する図（その2）である。

【図 13】本発明の通信手段を介したサービス提供システムにおける機器登録プロトコルを説明する図（その3）である。

【図 14】本発明の通信手段を介したサービス提供シス

テムにおける機器登録プロトコルを説明する図（その4）である。

【図 15】本発明の通信手段を介したサービス提供システムにおける機器登録プロトコルを説明する図（その5）である。

【図 16】本発明の通信手段を介したサービス提供システムにおける機器登録プロトコルを説明する図（その6）である。

【図 17】本発明の通信手段を介したサービス提供システムにおける機器登録プロトコルを説明する図（その7）である。

【図 18】本発明の通信手段を介したサービス提供システムにおける機器登録プロトコルを説明する図（その8）である。

【図 19】本発明の通信手段を介したサービス提供システムにおける機器認証プロトコルを説明する図（その1）である。

【図 20】本発明の通信手段を介したサービス提供システムにおいて適用可能な相互認証処理を説明する図である。

【図 21】本発明の通信手段を介したサービス提供システムにおける機器認証プロトコルを説明する図（その2）である。

【図 22】本発明の通信手段を介したサービス提供システムにおいて適用可能な相互認証処理を説明する図である。

【図 23】本発明の通信手段を介したサービス提供システムにおける機器認証プロトコルを説明する図（その3）である。

【図 24】本発明の通信手段を介したサービス提供システムにおける機器認証プロトコルを説明する図（その4）である。

【図 25】本発明の通信手段を介したサービス提供システムにおける利用者登録プロトコルを説明する図（その1）である。

【図 26】本発明の通信手段を介したサービス提供システムにおける利用者登録プロトコルを説明する図（その2）である。

【図 27】本発明の通信手段を介したサービス提供システムにおける利用者情報変更プロトコルを説明する図（その1）である。

【図 28】本発明の通信手段を介したサービス提供システムにおける利用者情報変更プロトコルを説明する図（その2）である。

【図 29】本発明の通信手段を介したサービス提供システムにおける利用者登録プロトコルを説明する図（その3）である。

【図 30】本発明の通信手段を介したサービス提供システムにおける利用者登録プロトコルを説明する図（その4）である。

【図 3 1】本発明の通信手段を介したサービス提供システムにおける利用者情報変更プロトコルを説明する図（その 3）である。

【図 3 2】本発明の通信手段を介したサービス提供システムにおける利用者情報変更プロトコルを説明する図（その 4）である。

【図 3 3】本発明の通信手段を介したサービス提供システムにおける利用者認証情報登録プロトコルを説明する図（その 1）である。

【図 3 4】本発明の通信手段を介したサービス提供システムにおける利用者認証情報登録プロトコルを説明する図（その 2）である。

【図 3 5】本発明の通信手段を介したサービス提供システムにおける利用者認証情報登録プロトコルを説明する図（その 3）である。

【図 3 6】本発明の通信手段を介したサービス提供システムにおける利用者認証情報登録プロトコルを説明する図（その 4）である。

【図 3 7】本発明の通信手段を介したサービス提供システムにおける利用者認証情報登録プロトコルを説明する図（その 5）である。

【図 3 8】本発明の通信手段を介したサービス提供システムにおける利用者認証情報登録プロトコルを説明する図（その 6）である。

【図 3 9】本発明の通信手段を介したサービス提供システムにおける利用者認証情報登録プロトコルを説明する図（その 7）である。

【図 4 0】本発明の通信手段を介したサービス提供システムにおける利用者認証情報登録プロトコルを説明する図（その 8）である。

【図 4 1】本発明の通信手段を介したサービス提供システムにおける利用者認証情報登録プロトコルを説明する図（その 9）である。

【図 4 2】本発明の通信手段を介したサービス提供システムにおける利用者認証情報登録プロトコルを説明する図（その 10）である。

【図 4 3】本発明の通信手段を介したサービス提供システムにおける利用者認証プロトコルを説明する図（その 1）である。

【図 4 4】本発明の通信手段を介したサービス提供システムにおける利用者認証プロトコルを説明する図（その 2）である。

【図 4 5】本発明の通信手段を介したサービス提供システムにおける利用者認証プロトコルを説明する図（その 3）である。

【図 4 6】本発明の通信手段を介したサービス提供システムにおける利用者認証プロトコルを説明する図（その 4）である。

【図 4 7】本発明の通信手段を介したサービス提供システムにおける利用者認証プロトコルを説明する図（その 5）である。

【図 4 8】本発明の通信手段を介したサービス提供システムにおける利用者認証プロトコルを説明する図（その 6）である。

【図 4 9】本発明の通信手段を介したサービス提供システムにおける利用者認証プロトコルを説明する図（その 7）である。

【図 5 0】本発明の通信手段を介したサービス提供システムにおける利用者認証プロトコルを説明する図（その 8）である。

【図 5 1】本発明の通信手段を介したサービス提供システムにおける利用者認証プロトコルを説明する図（その 9）である。

【図 5 2】本発明の通信手段を介したサービス提供システムにおける利用者認証プロトコルを説明する図（その 10）である。

【図 5 3】本発明の通信手段を介したサービス提供システムにおけるサービスプロトコルを説明する図（その 1）である。

【図 5 4】本発明の通信手段を介したサービス提供システムにおけるサービスプロトコルを説明する図（その 2）である。

【図 5 5】本発明の通信手段を介したサービス提供システムにおけるサービスプロトコルを説明する図（その 3）である。

【図 5 6】本発明の通信手段を介したサービス提供システムにおけるサービスプロトコルを説明する図（その 4）である。

【図 5 7】本発明の通信手段を介したサービス提供システムにおけるサービス提供例としての遠隔診断、修復処理を説明する図である。

【図 5 8】本発明の通信手段を介したサービス提供システムにおけるサービス提供例としてのバックアップ処理を説明する図である。

【図 5 9】本発明の通信手段を介したサービス提供システムにおけるサービス提供例としてのリストア処理を説明する図である。

【図 6 0】本発明の通信手段を介したサービス提供システムにおけるサービス提供例としてのデータ配信処理を説明する図である。

【図 6 1】本発明の通信手段を介したサービス提供システムにおけるサービス提供例としてのヘルプデータ提供処理を説明する図である。

【図 6 2】本発明の通信手段を介したサービス提供システムにおけるサービス提供例としてのチュートリアル処理を説明する図である。

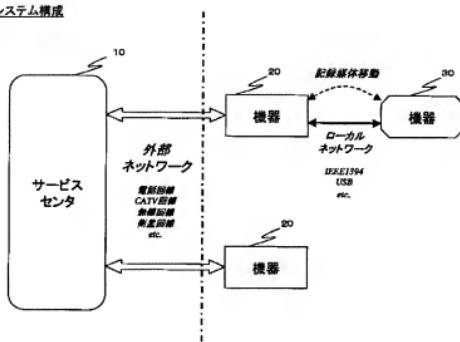
【符号の説明】

- 1 0 サービスセンタ
- 2 0 上位機器
- 3 0 制御対象機器(下位機器)

1 0 1	CPU	2 0 8	ローカルインタフェース
1 0 2	メモリ	2 0 9	操作部
1 0 3	サービス提供用データベース	2 1 0	記録装置
1 0 4	暗号化通信 I C	2 1 1	情報記録媒体
1 0 5	外部インタフェース	3 0 1	CPU
1 0 6	機器情報データベース	3 0 2	メモリ
1 0 7	利用者情報データベース	3 0 3	表示部
2 0 1	CPU	3 0 4	機器固有部
2 0 2	メモリ	3 0 5	暗号化通信 I C
2 0 3	表示部	3 0 6	記録媒体インターフェース
2 0 4	機器固有部	3 0 7	ローカルインタフェース
2 0 5	暗号化通信 I C	3 0 8	操作部
2 0 6	外部インタフェース	3 0 9	記録装置
2 0 7	記録媒体インターフェース	3 1 0	情報記録媒体

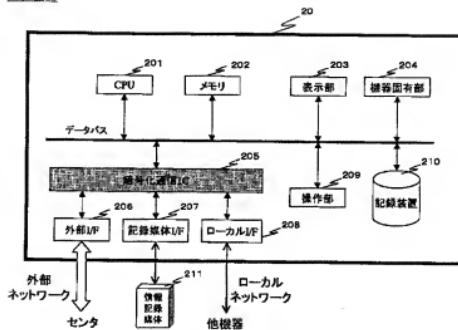
【図1】

システム構成



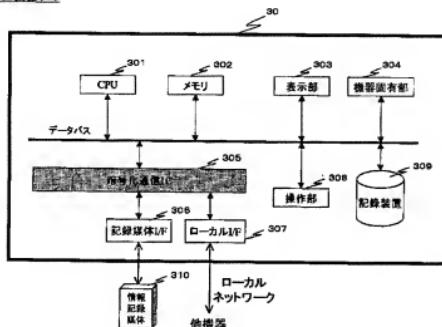
【図 2】

上位機器



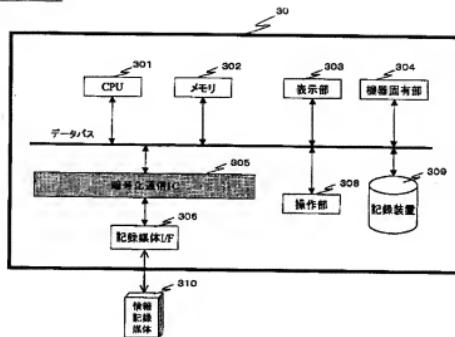
【図 3】

下位機器(1)



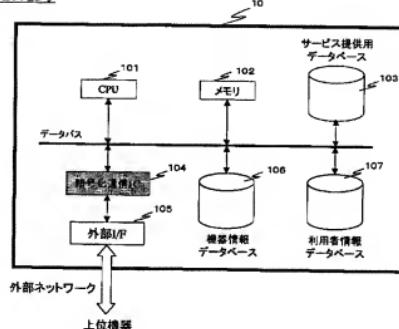
【図4】

下位機器(2)

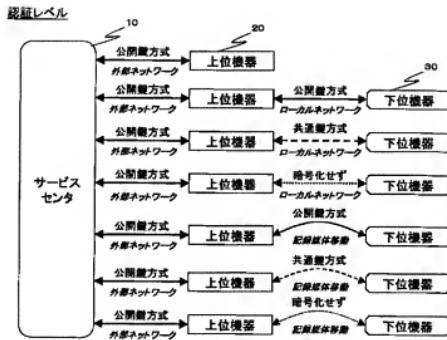


【図5】

サービスセンタ

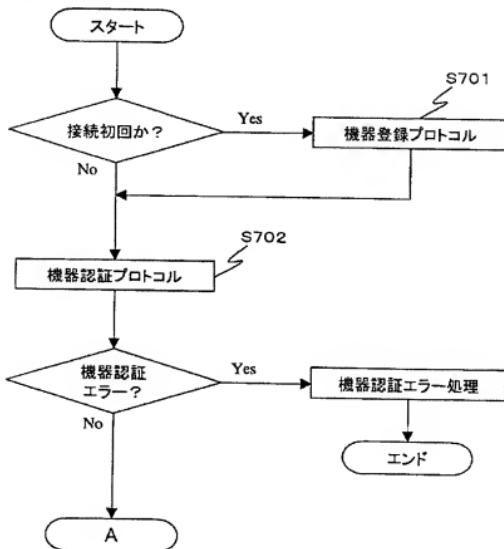


【図6】



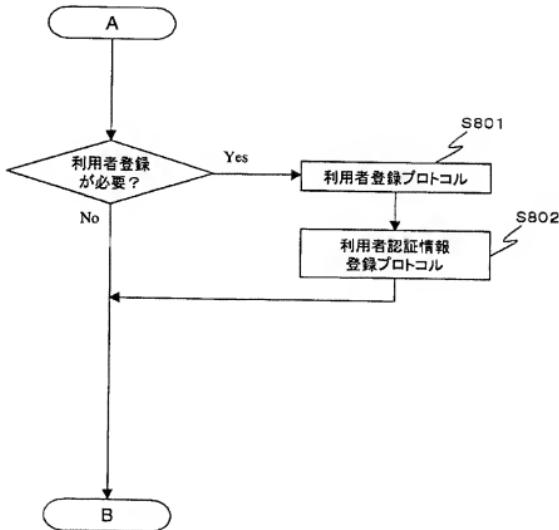
【図7】

全体フローーチャート 1

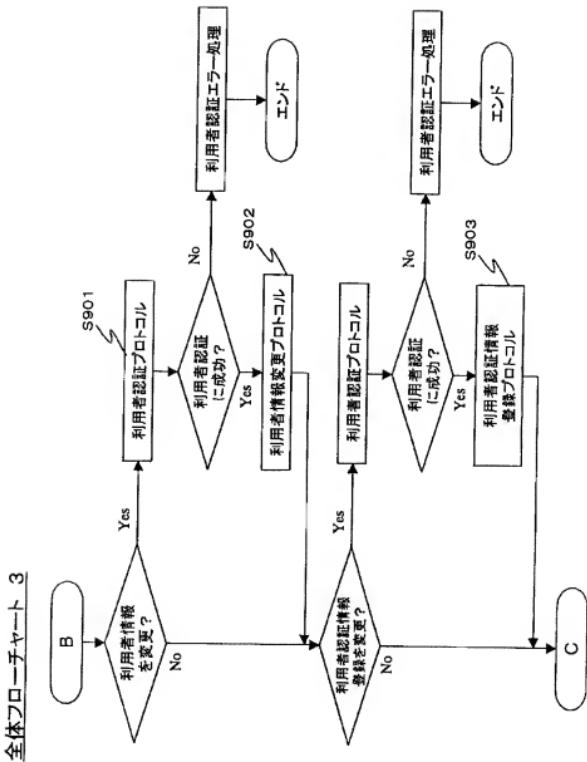


【図8】

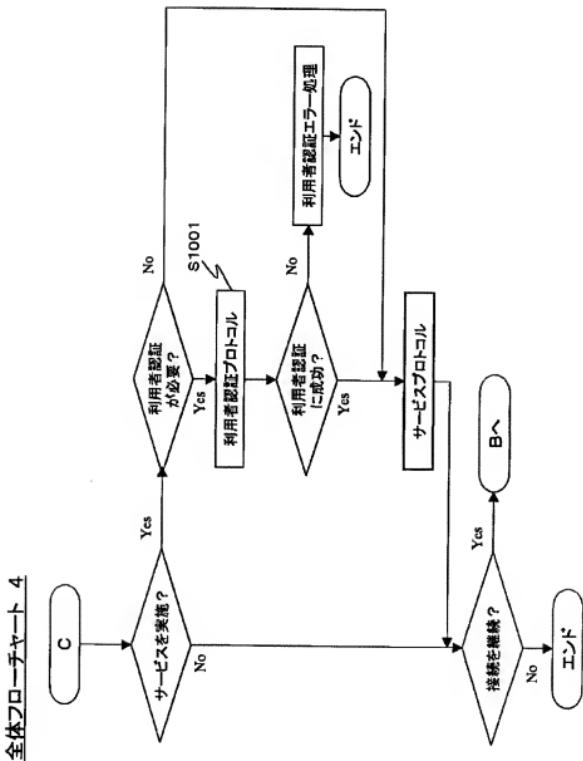
全体フローチャート 2



【図9】

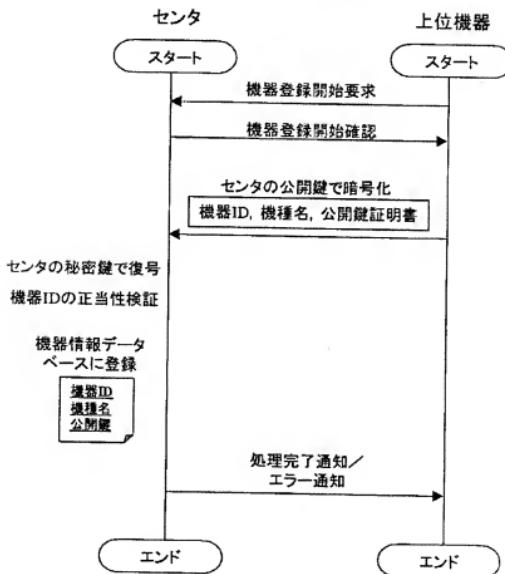


【図10】



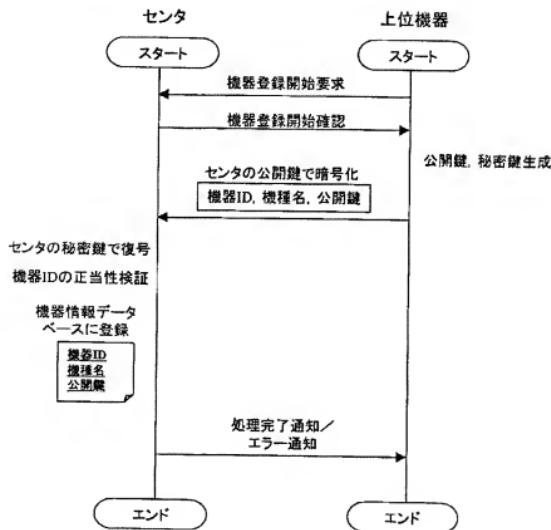
【図11】

機器登録プロトコル(1) 上位機器・鍵埋め込み



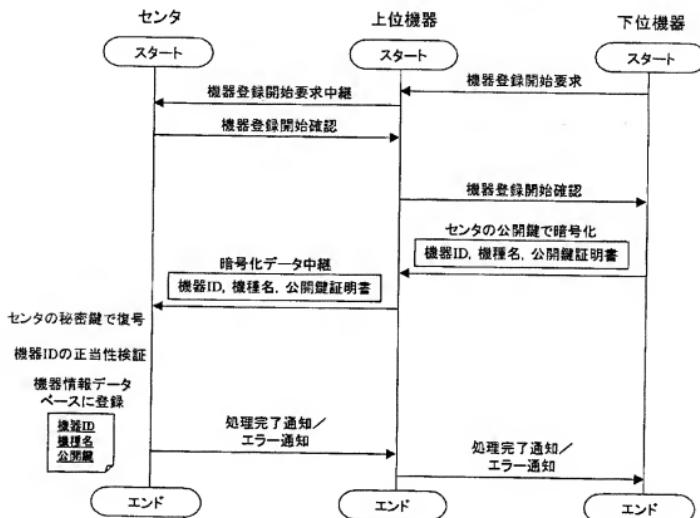
【図12】

機器登録プロトコル(2) 上位機器・鍵生成

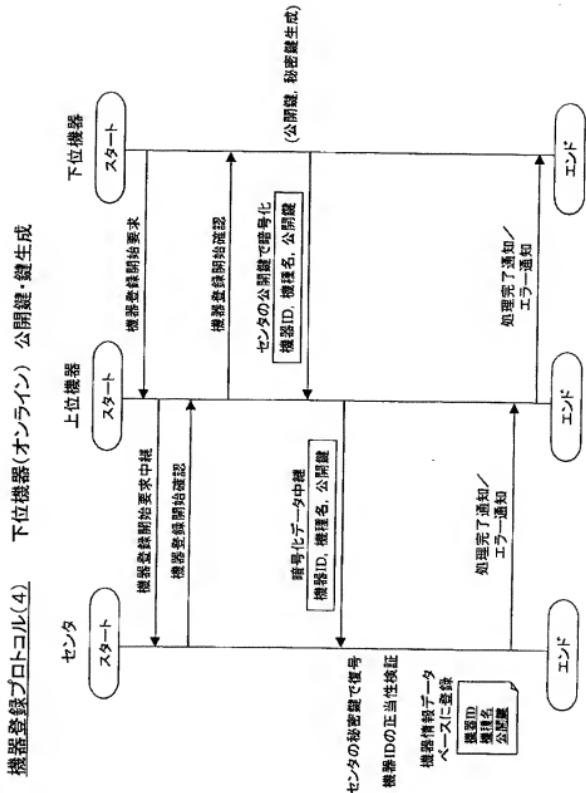


【図13】

機器登録プロトコル(3) 下位機器(オンライン) 公開鍵・鍵埋め込み

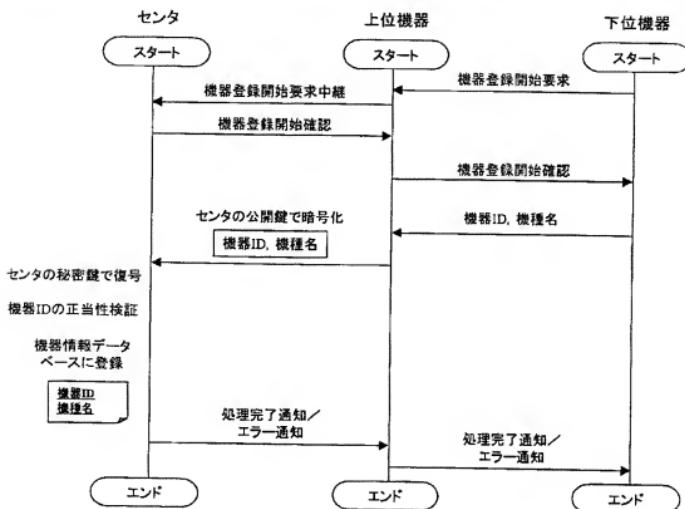


[図 1-4]

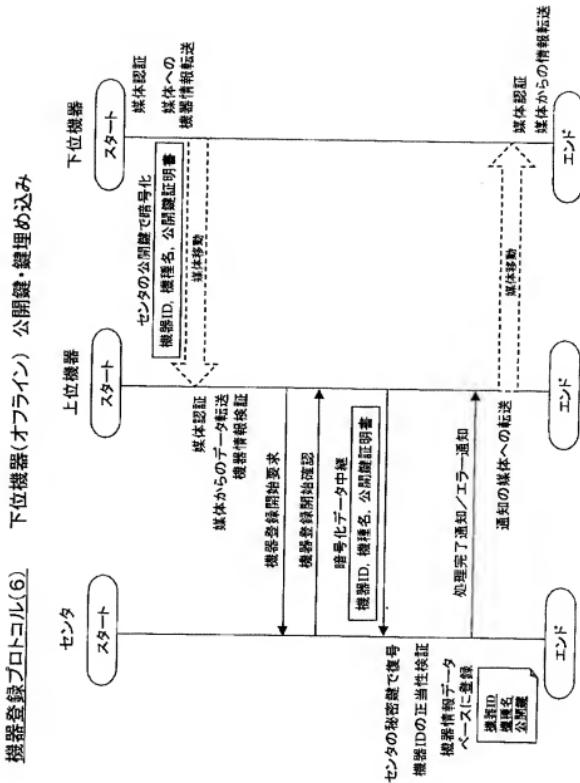


【図15】

機器登録プロトコル(5) 下位機器(オンライン) 共通鍵, 暗号化なし

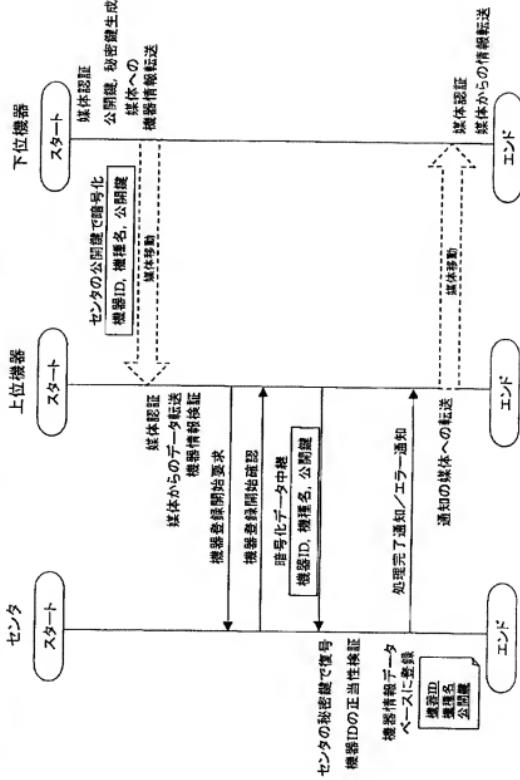


[図16]



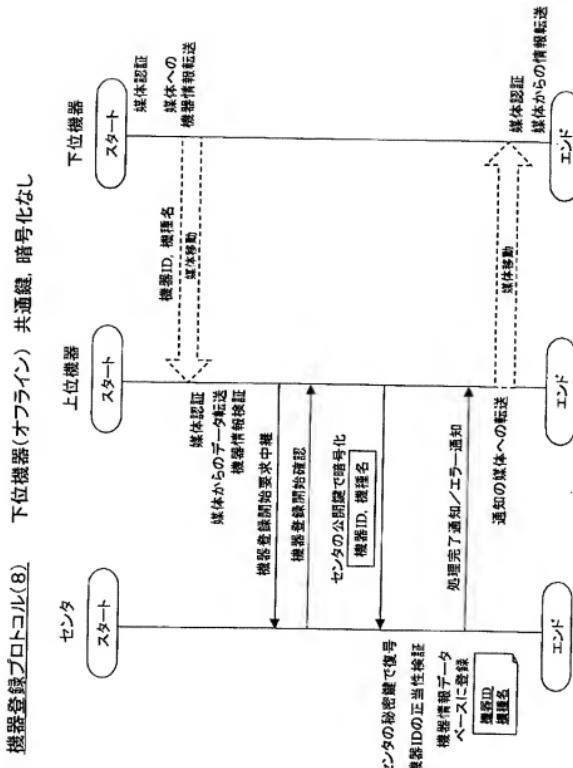
機器登録プロトコル(7)

下位機器(オフライン) 公開鍵・鍵生成



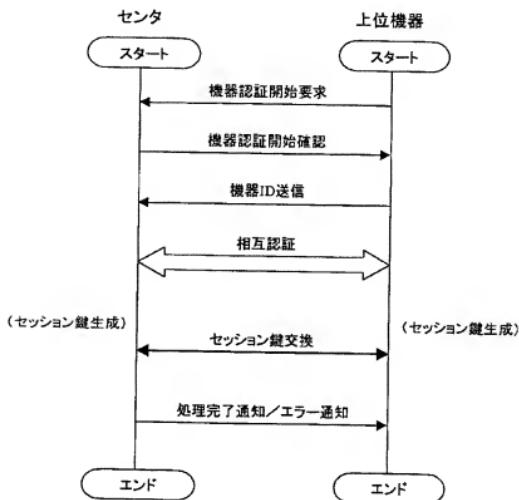
[図17]

【图 18】

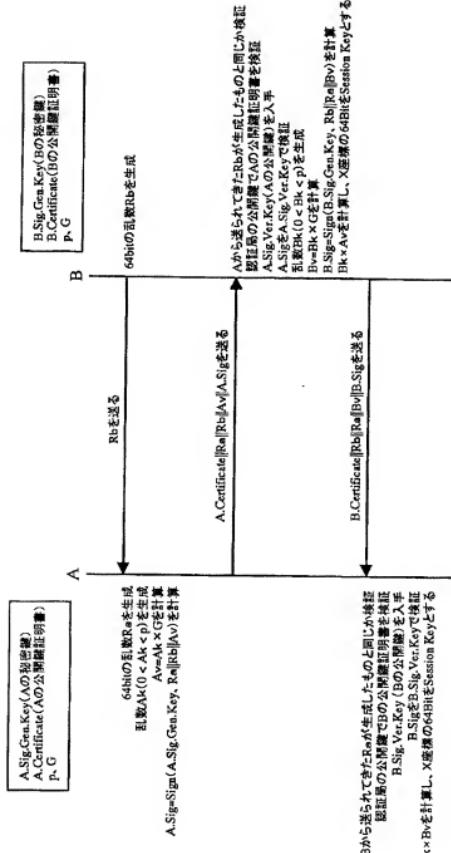


【図19】

機器認証プロトコル(1) センター上位機器

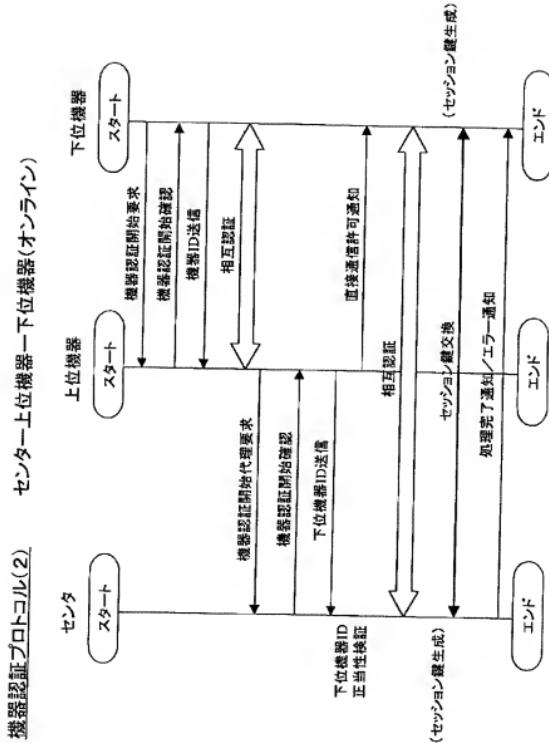


【図20】

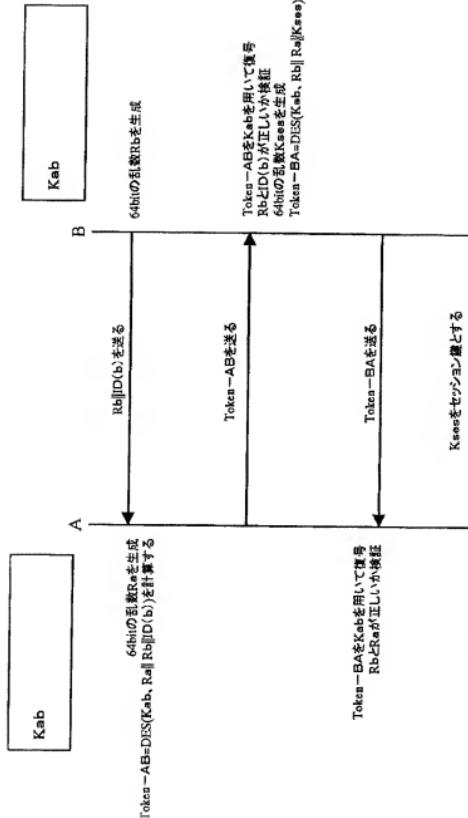


ISO/IEC 9798-3 非対称鍵暗号技術を用いた相互認証および鍵共有方式

[图21]



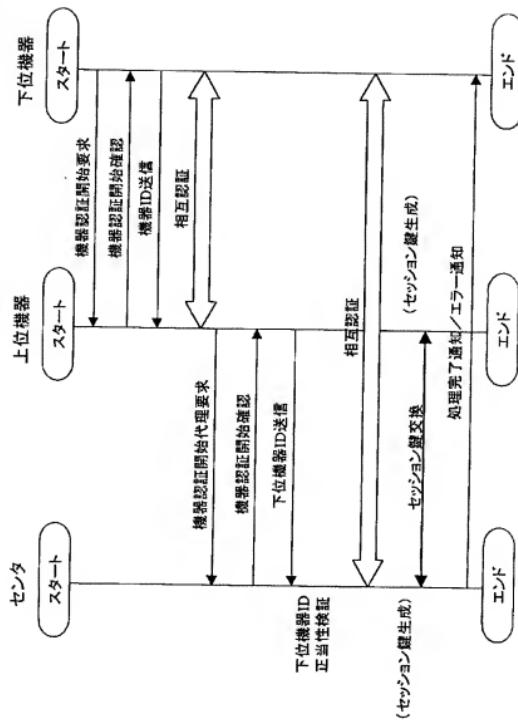
【図 2-2】



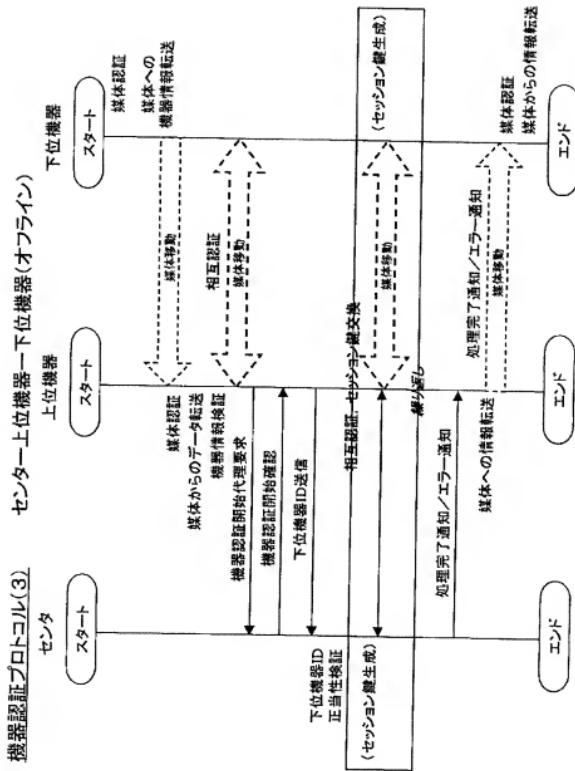
ISO/IEC 9798-2 対称鍵暗号技術を用いた相互認証および鍵共有方式

機器認証プロトコル(3)

センター上位機器一下位機器(オンライン／暗号化機能なし)

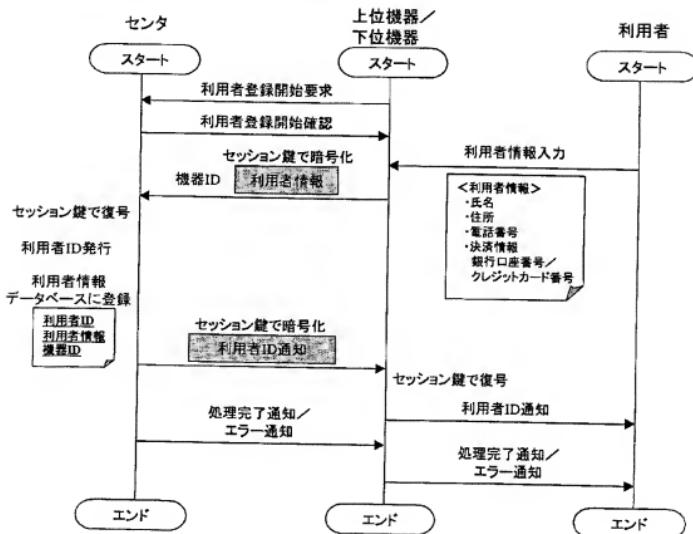


【图24】

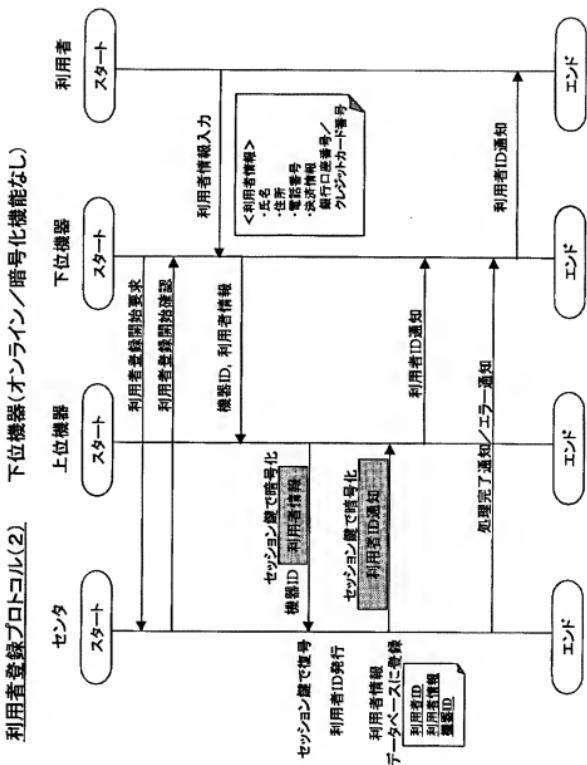


【図25】

利用者登録プロトコル(1) 上位機器、下位機器(オンライン)

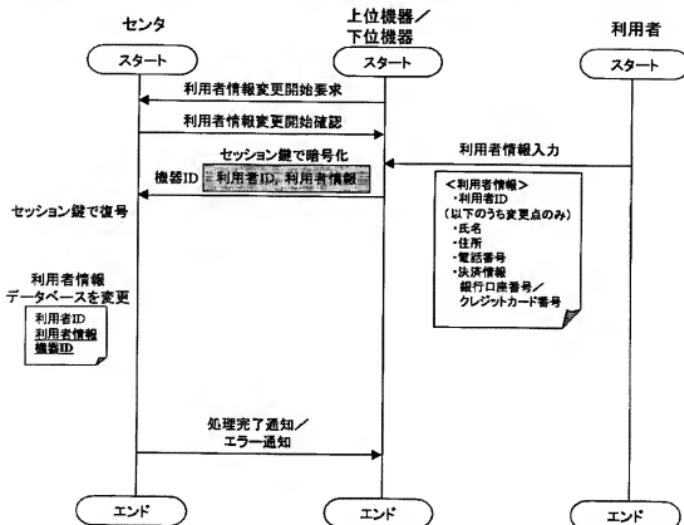


[図26]

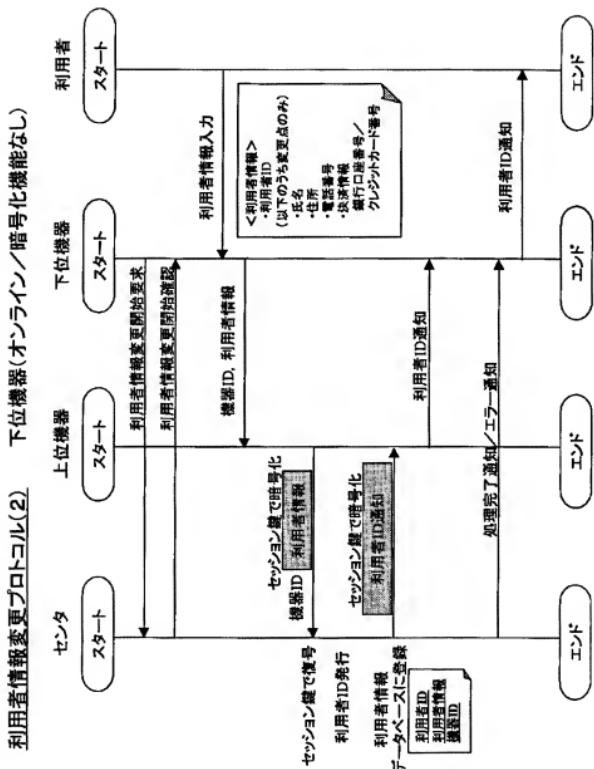


【図27】

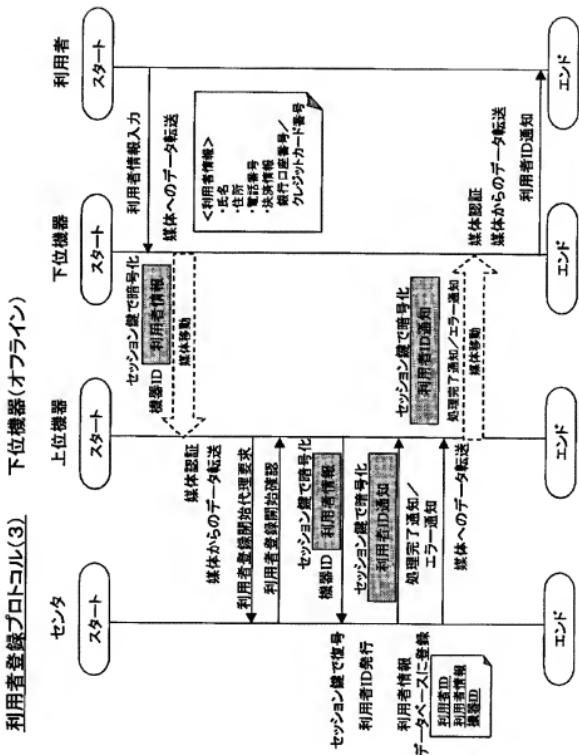
利用者情報変更プロトコル(1) 上位機器, 下位機器(オンライン)



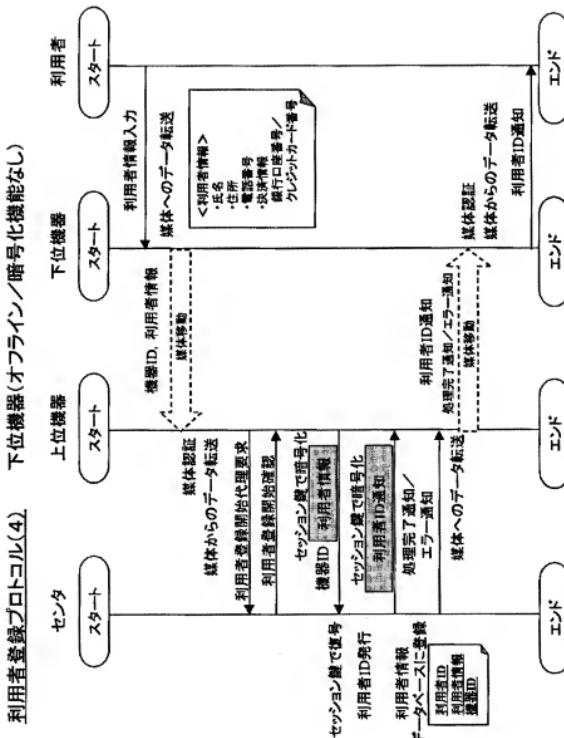
【図2.8】



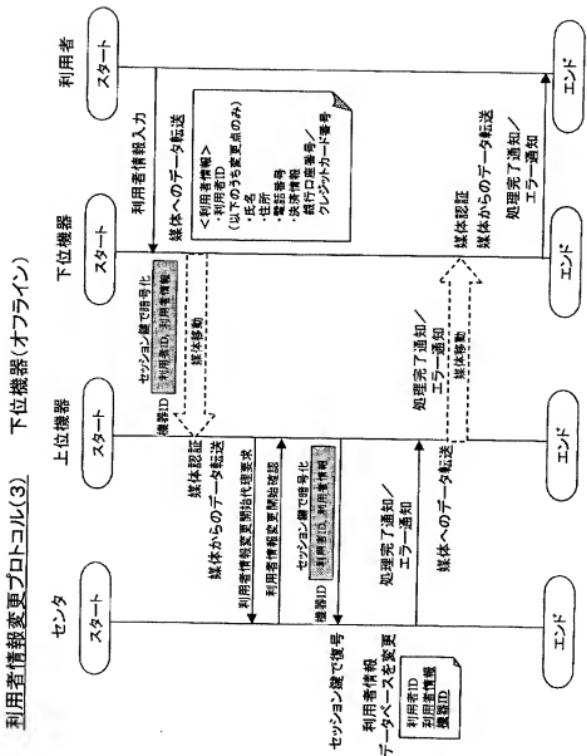
【图29】



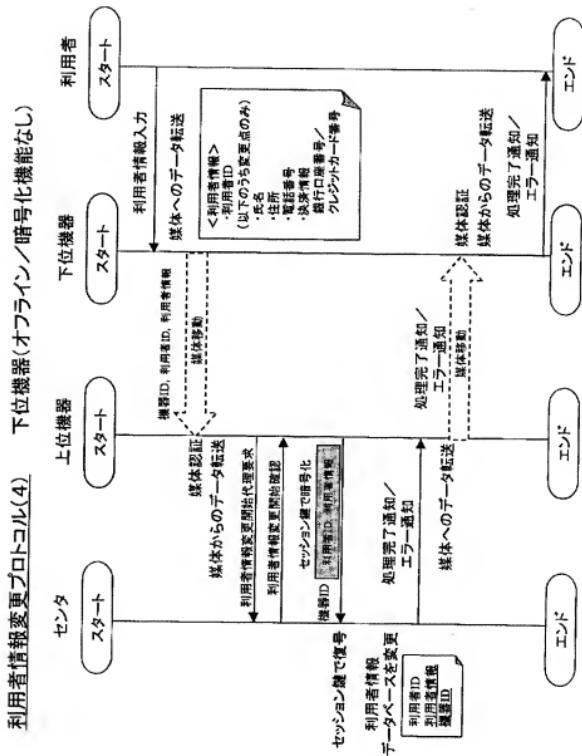
[図30]



[图31]

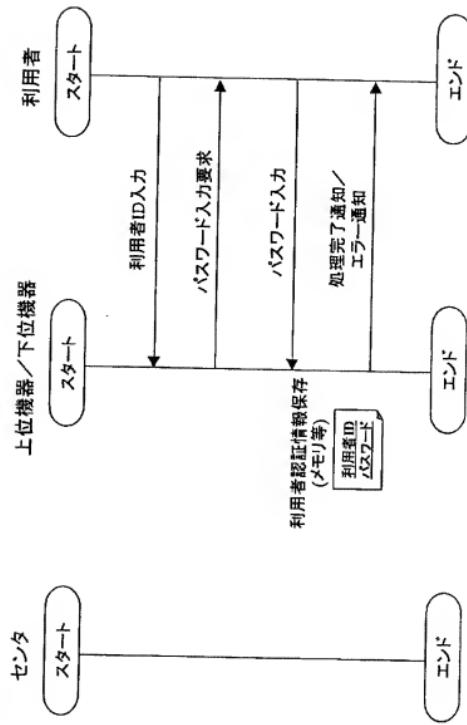


【図32】



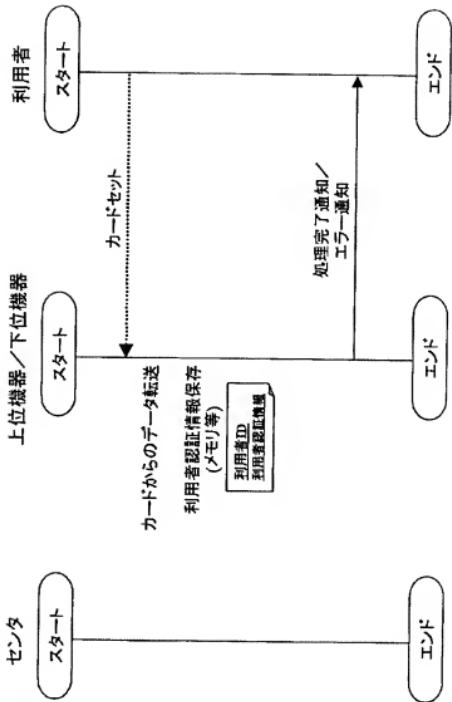
利用者認証情報登録プロトコル(1) パスワード(機器に保存)

【図33】

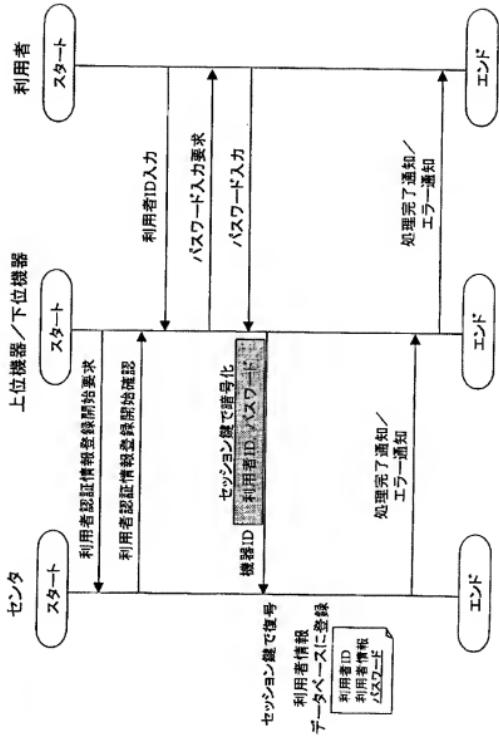


利用者認証情報登録プロトコル(2) IDカード(機器に保存) 上位機器・下位機器

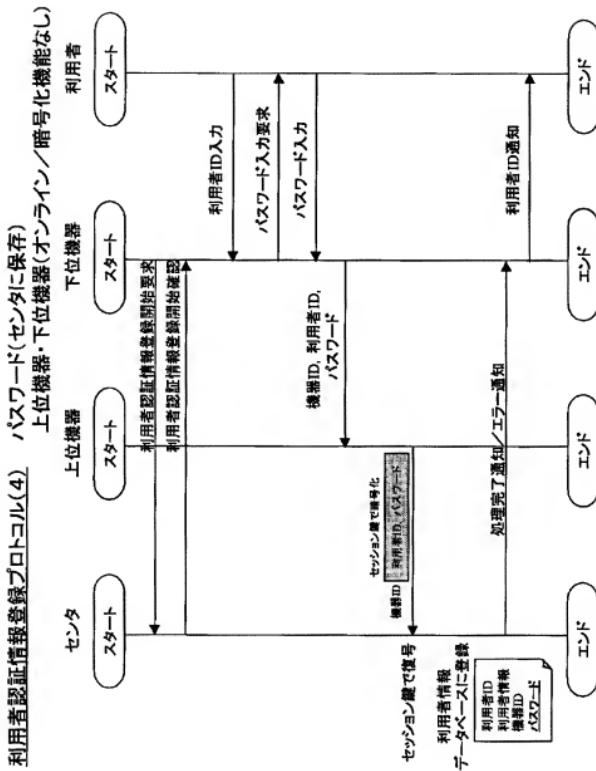
【図3-4】



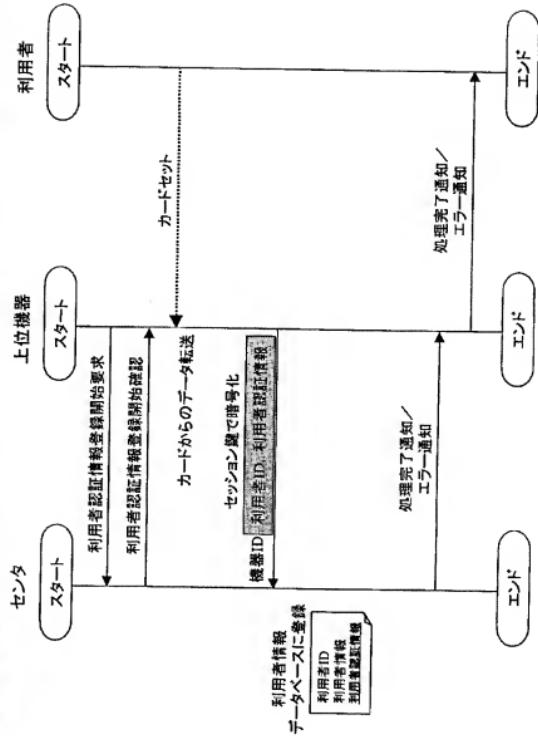
利用者認証情報登録プロトコル(3) パスワード(センタに保存) 上位機器・下位機器(オンライン)



【图36】

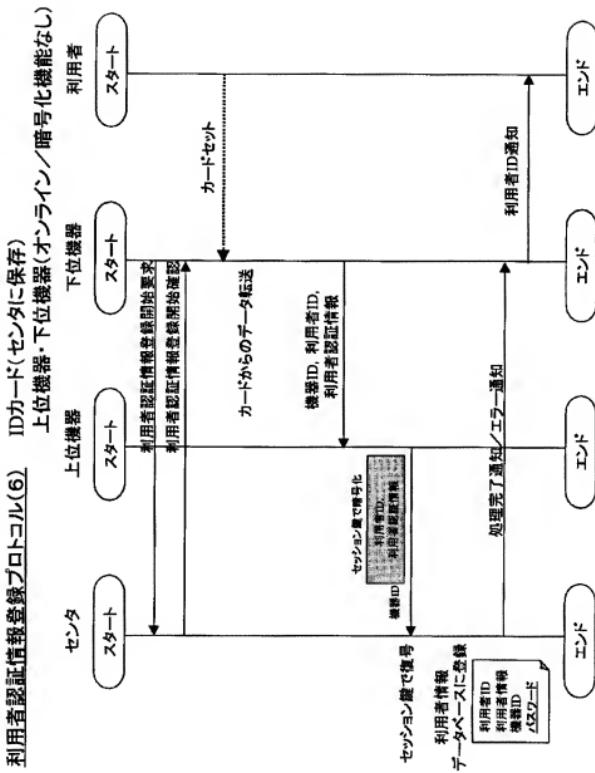


利用者認証情報登録プロトコル(5) IDカード(センタに保存) 上位機器・下位機器(オンライン)

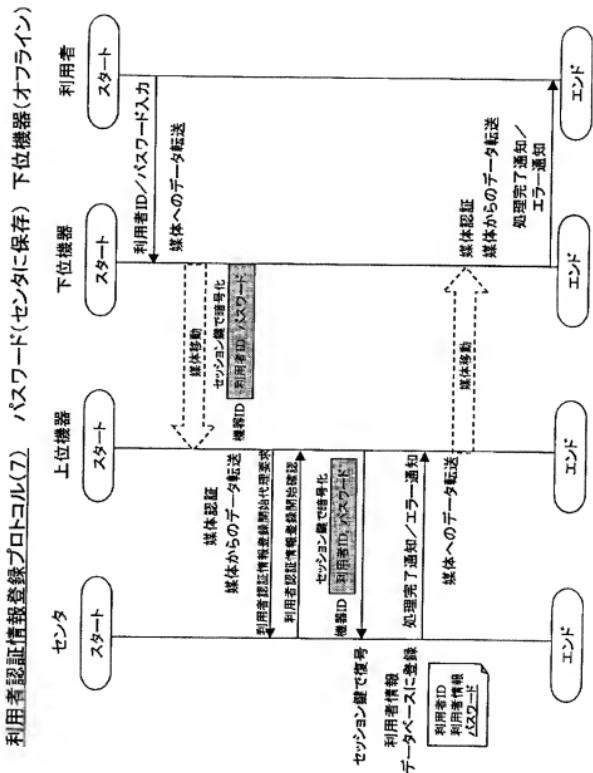


[图37]

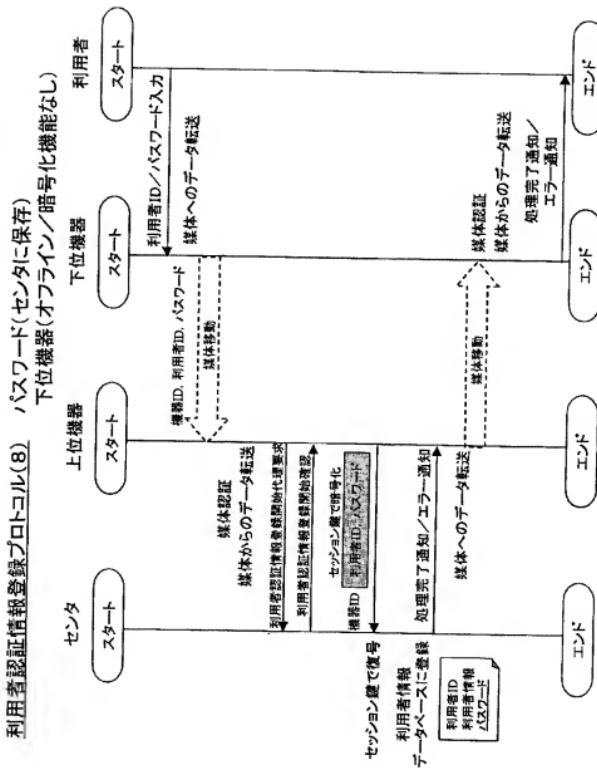
[図38]



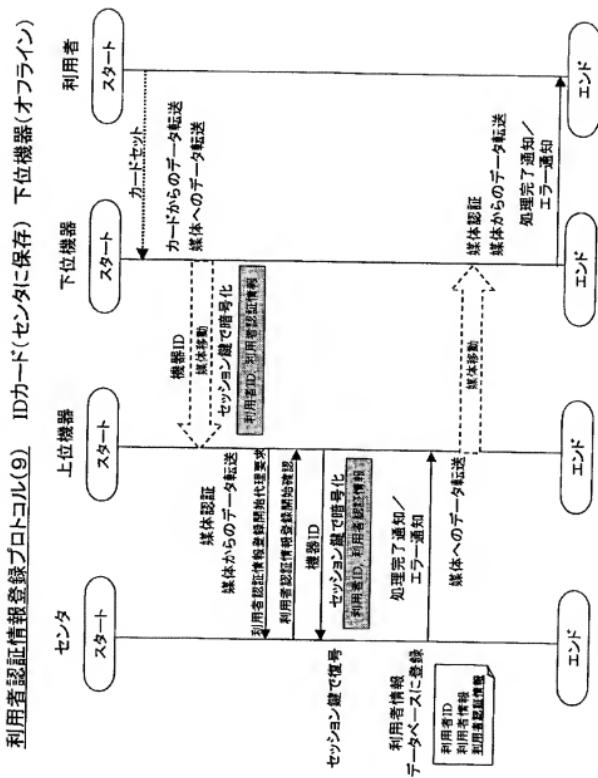
【图39】



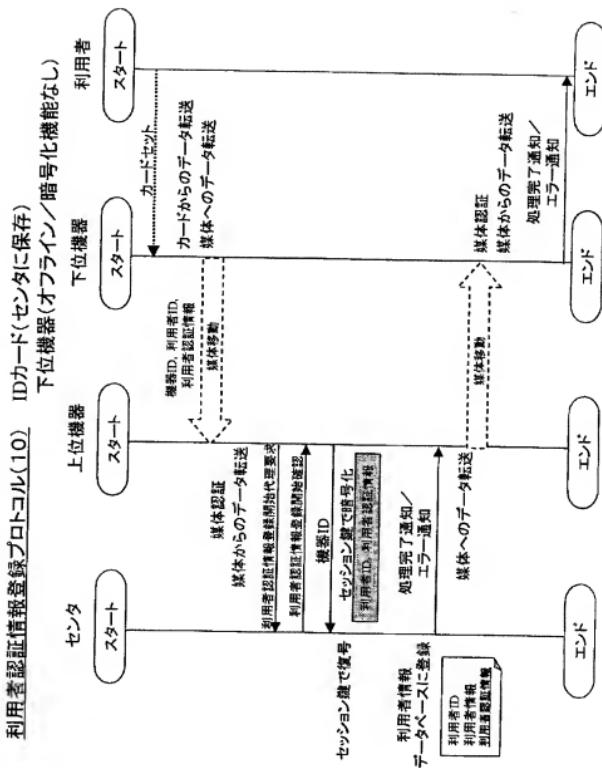
【图40】



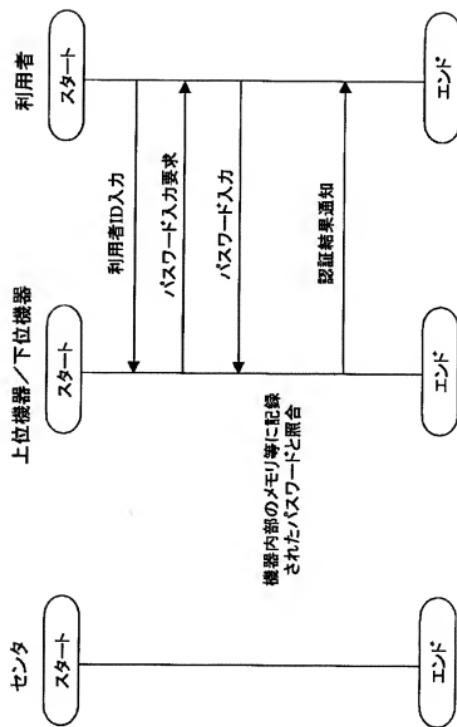
[図41]



【图42】

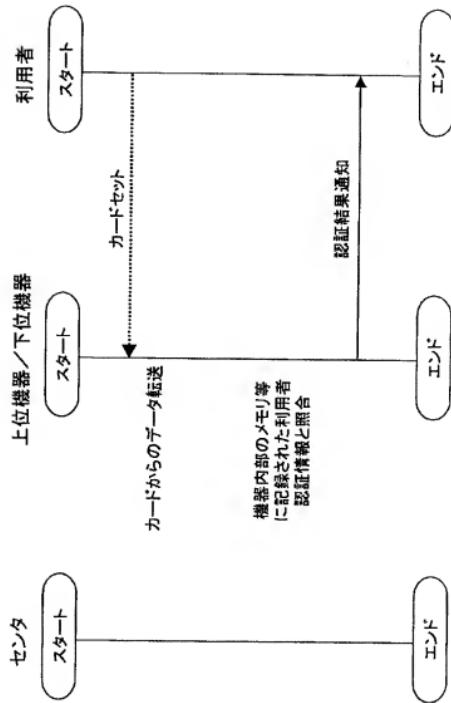


利用者認証プロトコル(1)
パスワード（機器に保存）



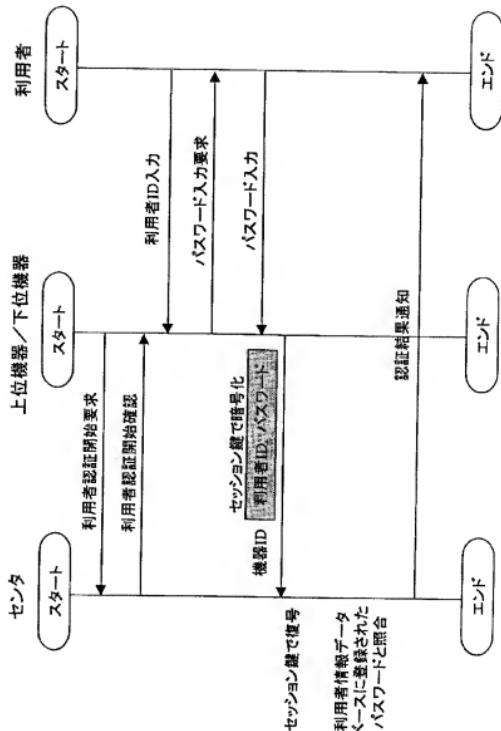
利用者認証プロトコル(2) IDカード(機器に保存) 上位機器・下位機器

利用者認証プロトコル(2) IDカード(機器に保存) 上位機器・下位機器

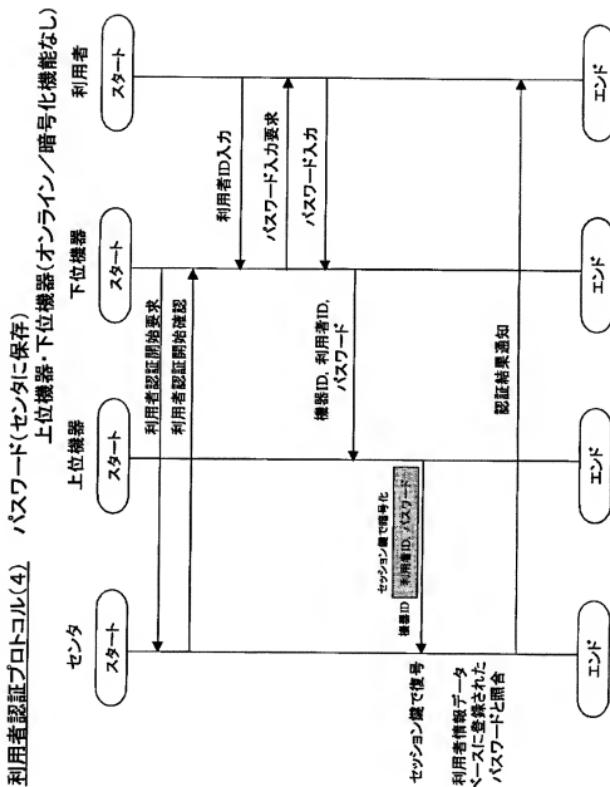


【図4-5】

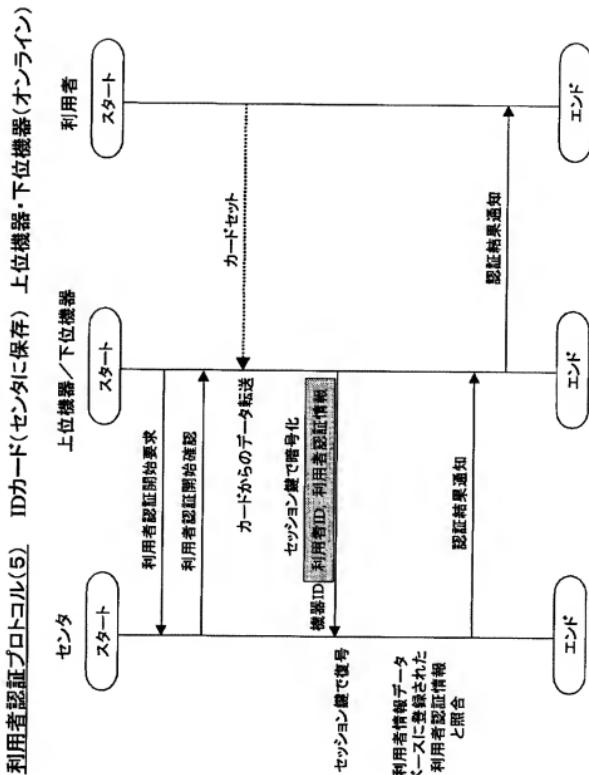
利用者認証プロトコル(3) パスワード(センタに保存) 上位機器・下位機器(オンライン)



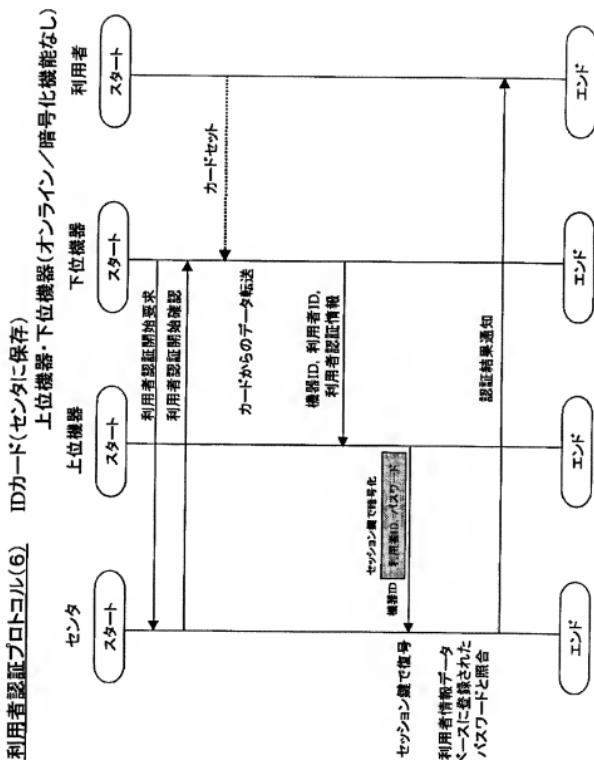
[図4-6]



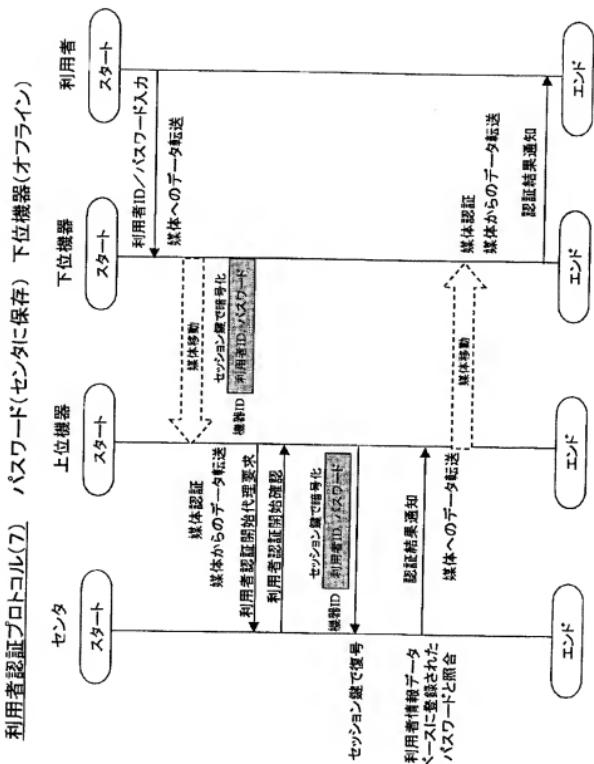
【図4-7】



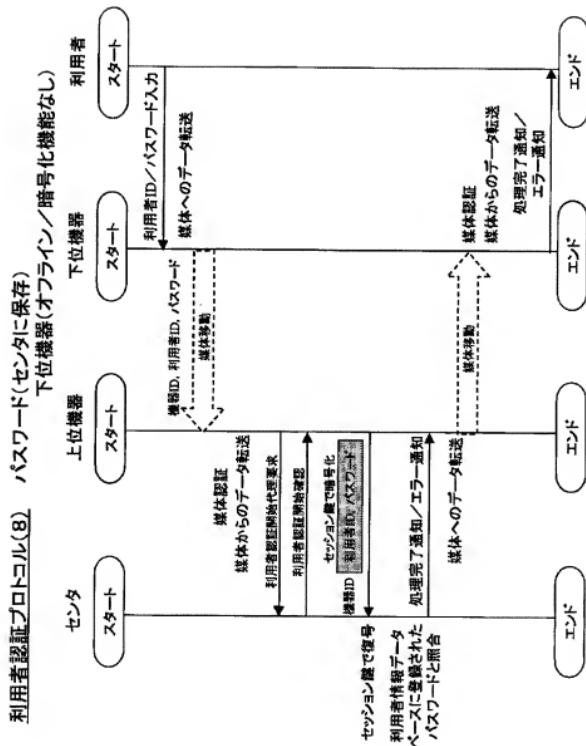
【図4-8】



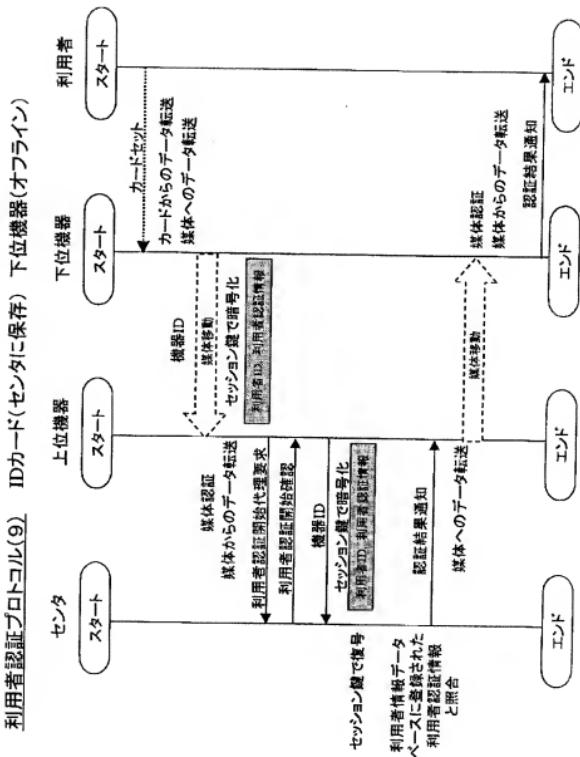
【图4-9】



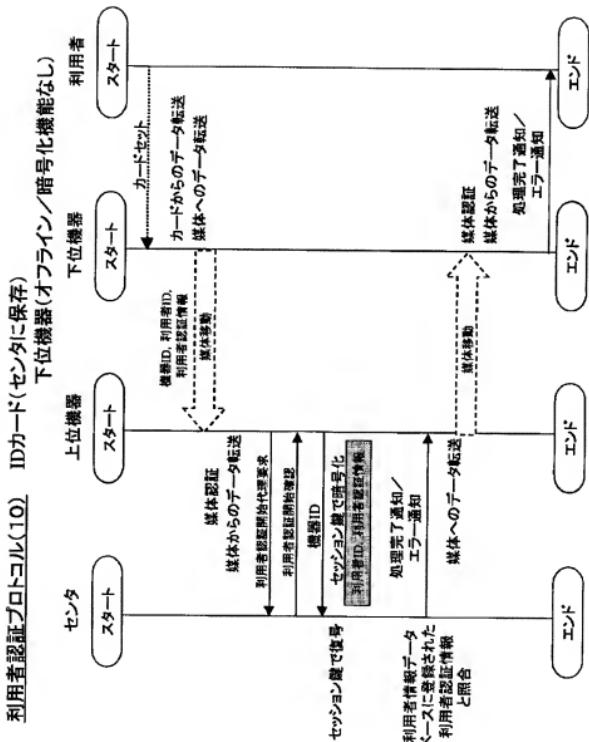
【図50】



【図51】

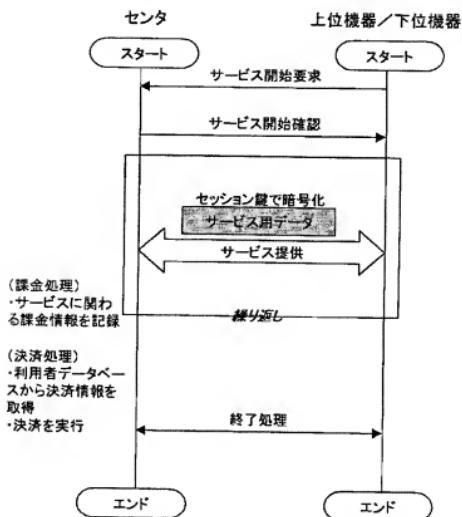


【图52】



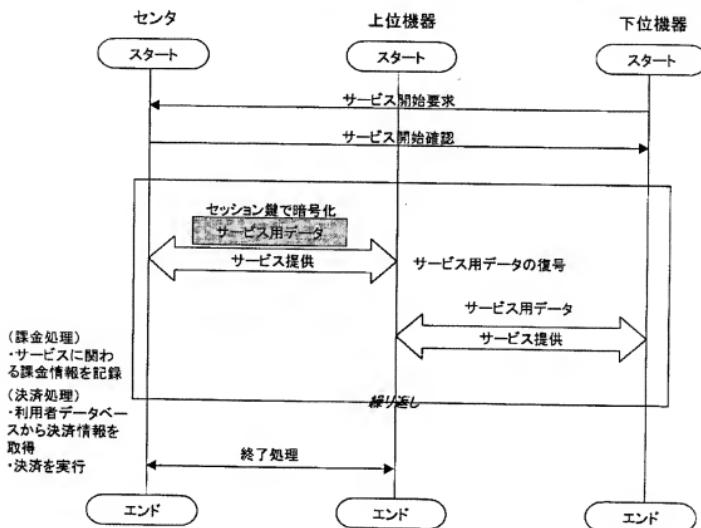
【図53】

サービスプロトコル(1) 上位機器、下位機器(オンライン)

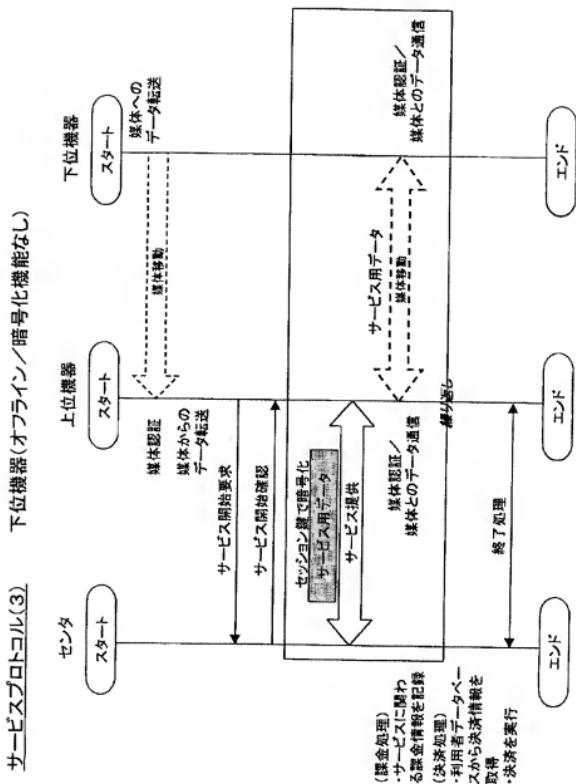


【図 5-4】

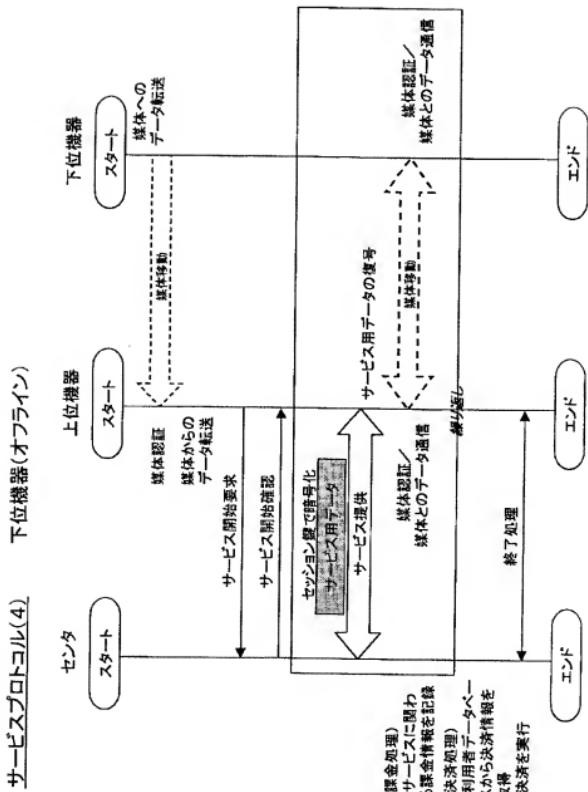
サービスプロトコル(2) 上位機器、下位機器(オンライン／暗号化機能なし)



【図55】

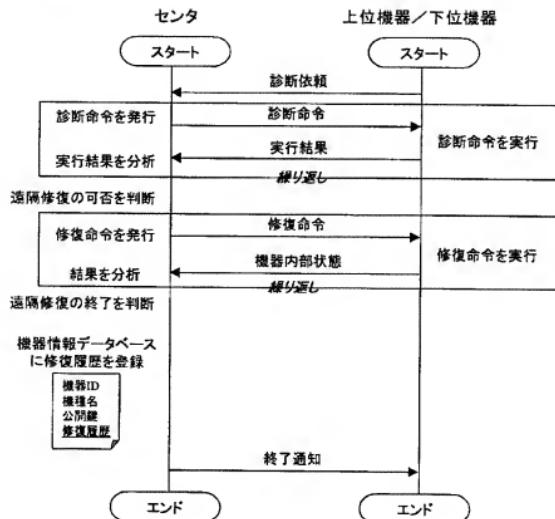


【図56】



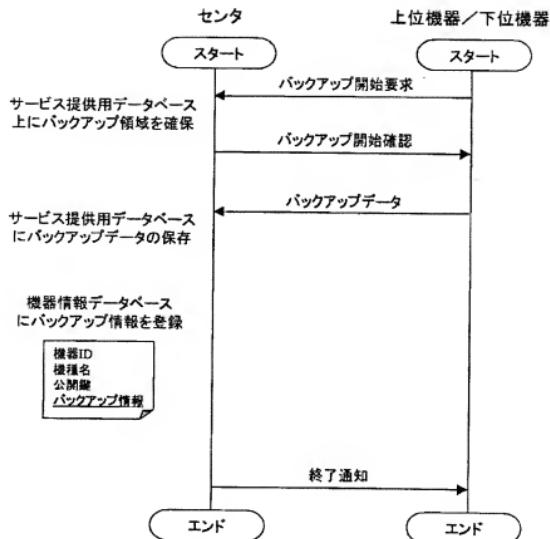
【図5-7】

遠隔診断・修復



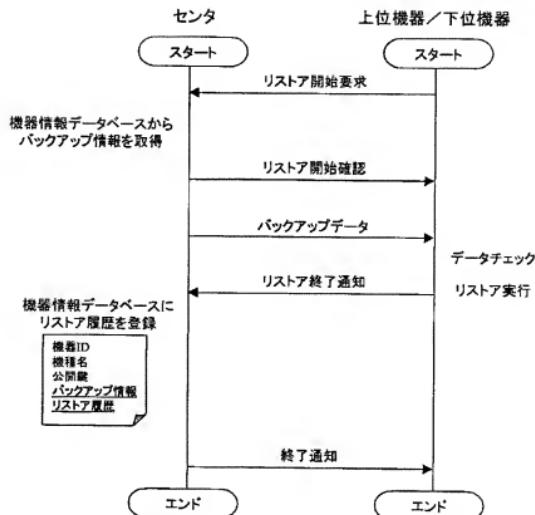
【図 5.8】

バックアップ



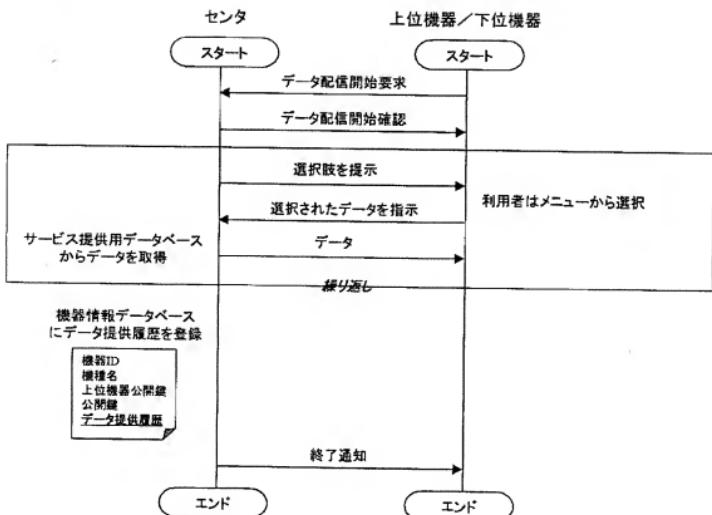
【図59】

リストア



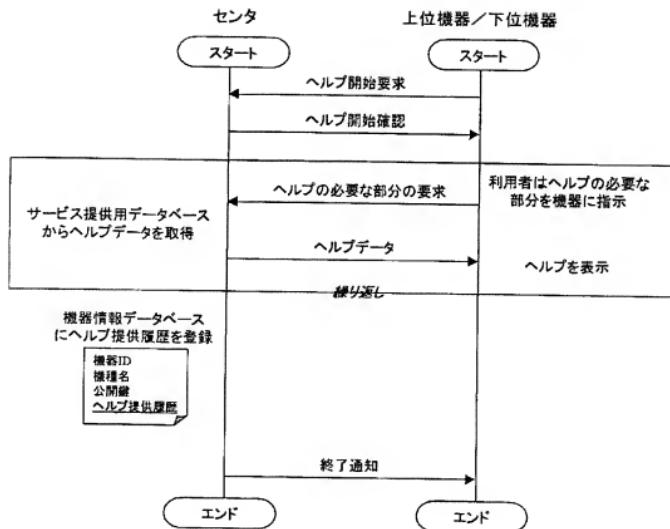
【図 6 0】

データ配信

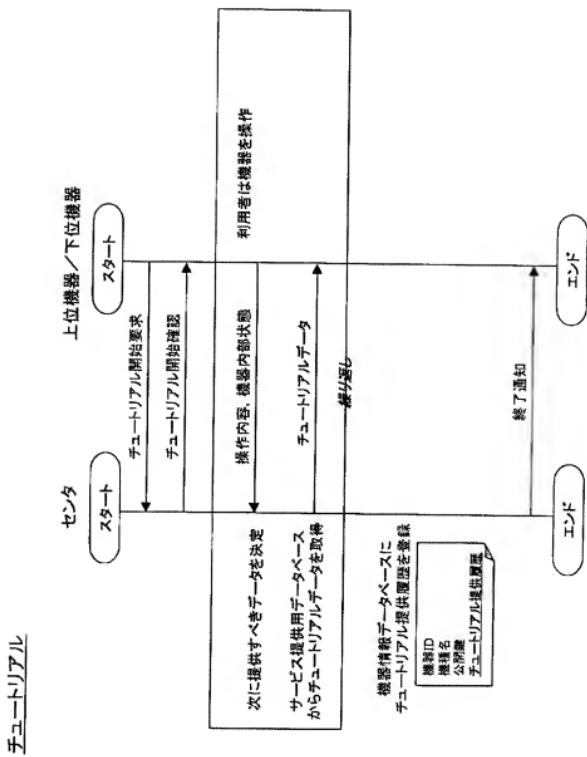


【図6.1】

ヘルプ



【図6-2】



フロントページの続き

(51) Int. Cl. 7	識別記号	F I	マーク (参考)
G 0 6 F 17/60	1 7 6	G 0 6 F 17/60	1 7 6 A 5 K 0 6 7
H 0 4 Q 7/38		H 0 4 B 7/26	1 0 9 R 9 A 0 0 1
H 0 4 L 9/32		H 0 4 L 9/00	6 7 3 B
12/66		11/20	B

(72)発明者　岡　誠
東京都品川区北品川6丁目7番35号　ソニ
一株式会社内

F ターム(参考) 5B049 AA05 BB00 BB46 CC03 CC22
CC36 CC39 CC48 DD04 EE03
EE05 EE23 EE56 GG04 GG07
GG10
5B085 AE23
5B089 HA01 HA06 HA11 JB14 JB19
KA12 KA17 KB13 KC58 KG03
KH30
5J104 AA07 KA02 KA04 KA05 NA03
5K030 GA15 HA05 HB04 HC01 HC14
HD01 HD06 JT09 LD20
5K067 AA30 BB04 DD17 EE02 EE16
HH11 HH24 HH36
9A001 CC03 C205 EE03 JJ01 JJ25
LL03